Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued April 22, 2011

Civil Service Commission

For the period July 1, 2008 through November 8, 2010

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The Civil Service Commission (CSC) is a quasi-judicial agency created under Chapter 7, Section 4I, of the Massachusetts General Laws. CSC has a five-member appellate board whose members are appointed by the Governor to five-year staggered terms. The powers and duties of CSC are detailed in Chapter 31, Section 2, of the General Laws. In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of information technology controls at CSC. Our audit, which covered the period July 1, 2008 through November 8, 2010, included a review of CSC's system access security, inventory control of computer equipment, business continuity planning, and selected controls regarding the protection of personal information per Executive Order 504 and Chapter 93H of the General Laws. In addition, we conducted a review of physical security and environmental protection.

Based on our review, we have concluded that, except for the issues addressed in the Audit Results section of this report, during the audit period ended November 8, 2010, CSC maintained adequate internal controls regarding system access security, inventory controls over computer equipment, business continuity planning, and selected controls regarding the protection of personal information.

Our audit determined that although CSC maintained an inventory of information technology (IT) resources and had performed an annual physical inventory in compliance with the requirements of the Office of the State Comptroller (OSC) it did not have formal policies and procedures in place for inventory control. Also, our audit disclosed that as a result of weak or nonexistent inventory control practices over IT resources, CSC did not properly account for all computer equipment in its inventory system of record. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. Moreover, we found that controls needed to be strengthened to provide prompt notification and updates of the inventory record when equipment is acquired, relocated, lost, or stolen.

Our review noted that the Commonwealth's Information Technology Division (ITD) provides disaster recovery services to CSC, and we confirmed that ITD provides off-site storage of electronic backup copies at state facilities as well as copies of magnetic media at a third-party vendor location for the systems used by CSC. However, we found that CSC did not have a formal, documented business continuity plan that would help ensure that mission-critical business operations can be recovered in a timely manner. Specifically, CSC did not develop or document contingency plans in the event of a potential loss of data processing. Contingency planning is an essential part of continuing an agency's business operations. As a result, CSC is vulnerable to a disruption of service should IT capabilities be rendered inoperable for an extended period of time.

INTRODUCTION

Background

The Civil Service Commission (CSC) is a quasi-judicial agency created under Chapter 7, Section 4I, of the Massachusetts General Laws. CSC has a five-member appellate board whose members are appointed by the Governor to five-year staggered terms. The powers and duties of CSC are detailed in Chapter 31, Section 2, of the General Laws.

The mission of CSC is to adjudicate appeals of public employees and job applicants under the civil service laws. CSC ensures that employment decisions are based on the employee's ability, knowledge, and skill level. It is CSC's responsibility to ensure that individuals who come before it are treated fairly and impartially. CSC is staffed by four full-time employees and three part-time employees.

The issues that come before CSC are mostly factual disputes dealing with whether an appointing authority has "just cause" to discipline or lay off an employee, or, in those cases involving appointments and promotions, whether there was reasonable justification to bypass the employee or job applicant. CSC has the authority to conduct investigations regarding the civil service process and review changes to the Personnel Administration Rules as proposed by the state's Human Resources Division.

The appeals process typically involves an appellant and an appointing authority. Appellants can represent themselves or they can be represented by an attorney, which occurs 75% to 80% of the time. A notice of the pre-hearing conference is sent out to both appellant and the appointing authority that informs both parties of what documents they need to bring to the pre-hearing conference. Turnaround time in regard to the notice is about a week maximum, sometimes sooner. Pre-hearings are held within 30 days of the original date the appeal was filed; full hearings, if necessary, are held 90 days thereafter.

CSC hears approximately 250 to 500 appeals annually. Over the past four years, CSC has reduced the number of pending appeals by approximately 78%, from 813 to 181. Hearings are held at the following locations: One Ashburton Place, Boston; Division of Administrative Law Appeals located at 98 North Washington Street, Boston; the State Office Building in Springfield; and the University

of Massachusetts School of Law located in North Dartmouth. CSC's budget for fiscal years 2009 and 2010 was $542,613 and $415,275, respectively.

CSC's Chairman, designated by the Governor, is responsible for the day-to-day operations of CSC and the assignment of cases to be heard by individual Commissioners or hearings officers. The appeals that are heard before CSC are input into a Microsoft Access database application called the Case Tracking System. The application system, which contains approximately 8,000 records, has the capability to track appeals and generate reports. The three types of appeals that come before CSC are bypass, disciplinary, and classification. The cases that come before CSC usually require a pre-hearing, and approximately 40% of all appeals that are filed result in a full hearing. The remaining cases are settled, withdrawn, or dismissed for lack of prosecution or on procedural and jurisdictional grounds.

Hearings are digitally recorded and uploaded to CSC's system once the hearings are completed, and the decision results are placed on CSC's website. CSC's files are hosted on file and printer servers located on the eighth floor at One Ashburton Place, Boston. Electronic backups are run nightly at One Ashburton Place as well as the Massachusetts Information Technology Center (MITC) in Chelsea. In addition, MITC sends out backup tapes (magnetic media) to an Iron Mountain location for off-site storage. Virtual Private Network access is given to employees who need to work in an off-site location, in the event an emergency occurs where employees cannot gain physical access to One Ashburton Place. CSC has a verbal agreement with the Division of Capital Asset Management to hold hearings at the State Office Building in Springfield when there is no physical access to One Ashburton Place.

CSC's networking services are provided by the Commonwealth's Information Technology Division (ITD), which allows the file server to be connected through the wide area network (WAN) to the MITC located in Chelsea, Massachusetts. The WAN allows access to the Massachusetts Management Accounting and Reporting System (MMARS), which is the Commonwealth's accounting system, and the Human Resources/Compensation Management System (HR/CMS). At the time of our audit, CSC's computer equipment consisted of 44 items, including 14 workstations, five laptops, seven printers, and various monitors, scanners, and digital recorders.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the General Laws, we performed an audit of information technology controls at CSC. Our audit was conducted from July 22, 2010 through November 8, 2010 and covered the period July 1, 2008 through November 8, 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the 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 a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit was also conducted in accordance with generally accepted industry practices. Criteria used in the audit included Chapter 93H of the General Laws; Executive Orders 490 and 504; Chapter 82 of the Acts of 2007; Chapter 647 of the Acts of 1989; management policies and procedures; and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association, July 2007. Our audit included a review of system access security, inventory controls over computer equipment, business continuity planning, and selected controls regarding the protection of personal information per Executive Order 504 and Chapter 93H of the General Laws. In addition, we conducted a review of physical security and environmental protection.

We determined whether system access security controls were in place to ensure that only authorized personnel had access privileges to the network and that controls over passwords were sufficient. We reviewed access to the mission-critical Case Tracking System application. We sought to determine whether adequate inventory controls were in place and in effect to properly record and safeguard computer equipment. We determined whether a business continuity plan was in place to provide detailed guidance for restoring mission-critical and essential business operations in a timely manner should the automated systems be unavailable for an extended period of time. Regarding personal information, we determined whether controls were in place to secure both electronic and hard copy records containing personal information. Furthermore, physical security and environmental protection controls in and around the agency were reviewed. In addition, we determined whether CSC employees had signed the "Information Technology User Responsibility Agreement" form as required, regarding protection of personal information and unacceptable use of the computer

To determine our audit scope and objectives, we initially obtained an understanding of CSC's mission and business objectives. To gain an understanding of the primary business functions that were supported by the automated systems, we conducted pre-audit interviews with management and reviewed CSC's enabling legislation, website, mission and business functions, and selected documents, such as CSC's "Internal Controls and Procedures" handbook. Through interviews, we gained an understanding of the information technology used to support CSC's business operations. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. A review of federal stimulus funds received through the American Recovery and Reinvestment Act (ARRA) was unnecessary, as CSC received no ARRA funding.

In conjunction with our audit, we reviewed IT-related policies and procedures for the areas under review and determined whether written, authorized, and approved policies and procedures had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, generally accepted control objectives for IT operations and security, and policy directives. Regarding our review of IT-related procedures, we interviewed the Chairman and General Counsel who oversee CSC's IT-related functions. We developed our audit scope and objectives based on our pre-audit work that included an understanding of CSC's mission, business objectives, and use of IT.

Our examination included a review of policies and procedures for authorizing, activating, and deactivating system access privileges to the local area network (LAN) and the mission-critical Case Tracking System. We also reviewed CSC's policies for password administration and password composition for access to the network. We determined whether all users who were authorized to access the CSC network were required to change their passwords periodically, and if so how often. To verify that CSC network users were also on the current payroll listing, a test was performed by cross referencing the list of network users against CSC's full time employee roster and any contract employees as of July 2010. In addition, a test was performed to ensure that all network users were authorized to access the network and had signed an "Information Technology User Responsibility" form.

To determine whether IT-related resources were being properly safeguarded and accounted for, we determined whether CSC had formal policies and procedures for inventory control and performed

tests, including tracing of items purchased to the inventory record, tracing items on the inventory record to the actual item and location, and verifying serial numbers and asset tag numbers.

We reviewed the inventory system of record to determine whether appropriate "data fields," such as serial identification number, asset tag number, manufacturer's model number, location, cost, and date of purchase, were included for each piece of equipment listed in the record and that sufficient information was provided to identify and account for the computer equipment. To determine whether the hardware inventory record accurately reflected computer equipment installed, we selected all 44 items (100%) listed on the inventory record for review. We compared the serial numbers and asset tag numbers of 20 IT equipment items listed on the inventory to the actual item itself. We then compared the serial number and asset tag number of the items to the hardware inventory record. We determined whether the serial numbers and asset tag numbers were accurately recorded on the inventory record. We identified IT purchases and determined whether they were properly recorded on the inventory record. We sought to determine whether CSC was in compliance with the reporting of missing or stolen assets as required by Chapter 647 of the Acts of 1989. We interviewed senior management to determine whether any IT equipment had been lost, stolen, or put into surplus during the audit period. In addition, we sought to determine whether CSC had a software inventory.

To assess business continuity planning, we sought to determine whether a formal business continuity plan was in place that would include both disaster recovery and business continuity strategies to restore mission-critical and essential operations and enable CSC to continue its daily operations in a timely manner should the automated systems be unavailable for an extended period. We gained an understanding of CSC's IT infrastructure and interviewed the Chairman and General Council to determine whether the criticality of the application system had been assessed, and if the risks and exposures to CSC's computer operations had been evaluated. The adequacy of controls were evaluated to ensure the copies of data files residing on CSC's server would be available for recovering automated systems and network services. We interviewed the Information Technology Division personnel responsible for CSC's disaster recovery regarding electronic backups of mission-critical applications and the generation and storage of backup copies of magnetic media. We performed a walk-through of the Information Technology Division's server room on the 8th floor of One Ashburton Place, Boston and reviewed physical security and environmental protection controls over the site as well as performed a review of the adequacy of provisions for off-site storage

of backup copies of electronic and magnetic media. We also determined what controls CSC had in place to secure both electronic and hardcopies of personal information. Furthermore, physical security and environmental protection controls in and around the agency were reviewed.

Based on our review, we have concluded that, except for the issues addressed in the Audit Results section of this report, during the audit period ended November 8, 2010, CSC maintained adequate internal controls regarding system access security, inventory controls over computer equipment, business continuity planning, and selected controls regarding the protection of personal information.

AUDIT RESULTS

1. INVENTORY CONTROLS OVER COMPUTER EQUIPMENT

Our audit determined that although the Civil Service Commission (CSC) maintained an inventory of information technology (IT) resources and had performed an annual physical inventory in compliance with the requirements of the Office of the State Comptroller (OSC); it did not have formal policies and procedures in place for inventory control. Also, our audit disclosed that as a result of weak or nonexistent inventory control practices over IT resources, CSC did not properly account for all computer equipment in its inventory system of record. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. Moreover, we found that controls needed to be strengthened to provide prompt notification and updates of the inventory record when equipment is acquired, relocated, lost, or stolen. The absence of a sufficiently reliable inventory of computer equipment hinders CSC's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and support IT configuration management objectives.

The OSC requires that agencies have formal policies and procedures in place regarding inventory, including the purchasing, tagging, and recording of assets specifying date of purchase and cost, lost or stolen equipment, disposal and surplus of assets, and the performance of an annual physical inventory. Our analysis of CSC's inventory indicated that although most of the appropriate data fields, such as description, identification tag, user name, serial number, and location, were present, the listing lacked data fields for cost and date of purchase. The OSC requires all departments to record the cost and date of purchase in inventory systems of record is in order to provide a comprehensive, auditable inventory record of fixed assets.

Our audit revealed that serial numbers could be verified for only 14 out of 44 IT-related items when the inventory list was compared to the actual items on hand. CSC's lack of a complete hardware inventory listing hinders CSC's ability to properly account for available hardware equipment and undermines its ability to detect missing or stolen equipment. CSC needs to ensure that appropriate controls are in place and in effect for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory database.

Our audit disclosed that CSC did not report to the Office of the State Auditor (OSA) a missing laptop computer. Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies, requires agencies to immediately report unaccounted-for variances, losses, shortages, or thefts of funds or property to the OSA. A test of the July 23, 2010 inventory of computer hardware revealed that a Dell laptop assigned to a former employee could not be located. The laptop, a Dell D600, was assigned to a former employee who left CSC around the end of April, 2010. The Chairman was not aware of the requirement to report lost or stolen equipment to the OSA. When it was brought to the attention of the Chairman, the missing laptop was then reported to the OSA.

An inspection of two similar laptops revealed that they were several years old and could not be started. According to CSC's Chairman, the purchase of these laptops preceded his appointment to CSC approximately five years ago, and he intends to surplus these outdated and non-functional laptops. Generally accepted industry standards and sound management practices require that adequate controls be incorporated to account for and safeguard fixed assets against theft, loss, or misuse.

Recommendation

CSC should:

- Develop and implement internal control policies, procedures, and practices regarding inventory control of IT resources in the areas of recording and inventory verification to help ensure that CSC properly accounts for its computer equipment. CSC should implement appropriate assurance methods, such as independent verification, physical inspection, reconciliation, and oversight to ensure that inventory controls are in place and in effect.

- Adapt its current Internal Controls and Procedures guidelines to comply with the OSC's Internal Control Guide for Departments regarding asset management. Once senior management has approved the policies and procedures, the policies and procedures should be distributed and instructed to the appropriate staff.

- Enhance its inventory control policies and procedures to ensure that all data fields required by the OSC are entered on CSC's inventory list. Specifically, we recommend that the data fields in the IT inventory be expanded to include the cost and date of purchase for the computer equipment and that all other fields be verified, especially the serial number field.

- Implement these control procedures to help ensure that all IT-related equipment is recorded on the inventory record in a complete, timely, and accurate manner so that CSC can generate a complete record of all computer equipment on a perpetual basis. The perpetual inventory record of IT resources should be periodically verified through reconciliation to computer

equipment acquisition, records of lost or stolen equipment, and disposal records. CSC's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items that may be held in storage.

- Maintain policies and procedures that will comply with Chapter 647 of the Acts of 1989 and immediately report all instances of unaccounted for variances, losses, and thefts of funds or property to the Office of the State Auditor.

- Ensure that all obsolete and non-functional IT equipment is surplused and removed from the inventory system of record.

Auditee's Response

In regard to those areas where the Audit recommends improvements, we have already taken steps to implement some of those recommendations and plan on implementing all of the recommendations by the end of this fiscal year (June 30, 2011).

We concur with the overall findings and conclusions of the audit that: 1) As captured in the case tracking system, the Commission has reduced the number of appeals pending by 78%, from 813 to 181, over the past four years; 2) the Commission has adequate internal controls in place regarding system access security and physical security; 3) the Commission maintains a detailed internal controls and procedures manual; and 4) the Commission maintains an inventory of all IT equipment that is updated annually.

We concur with the audit's conclusion that the Commission maintains an inventory of all IT equipment that is updated annually. As a result of operating on a shoe-string budget, the Commission's IT inventory includes outdated IT equipment (i.e. – laptops purchased over seven years ago; used desktops purchased two years ago; used printers that appear to have been informally acquired by the Commission from other agencies over the years). As a result, the date of acquisition is often unknown and in some cases, the equipment does not have the identifying information that the audit recommends capturing.

Where possible, however, we have taken or will take steps to comply with most of the recommendations in this section as follows:

1. *A request has been submitted to ANF's centralized IT division to surplus all of the remaining laptop computers that were purchased approximately seven years ago. They are obsolete and no longer serve any useful function.*
2. *The Commission's Internal Controls and Procedures Manual has been updated and now includes information regarding the need to promptly report any lost or stolen equipment to the Auditor's Office, pursuant to Chapter 647 of the Acts of 1989.*
3. *Within 30 days, the IT inventory spreadsheet will be updated with the additional fields suggested in the Audit and a further inspection of all IT equipment will be conducted to capture, when available, accurate tag and serial numbers and, when available, the date of acquisition.*
4. *Prior to June 30, 2011, the Internal Controls and Procedures Manual will be updated to formalize the current practices regarding inventory verification and reconciliation to conform with the Internal Control Guide of the Office of the State Comptroller.*

2. BUSINESS CONTINUITY PLANNING

Our review noted that the Commonwealth's Information Technology Division (ITD) provides disaster recovery services to CSC, and we confirmed that ITD provides off-site storage of electronic backup copies at state facilities as well as copies of magnetic media at a third-party vendor location for the systems used by CSC. However, we found that CSC did not have a formal, documented business continuity plan that would help ensure that mission-critical business operations can be recovered in a timely manner. Specifically, CSC did not develop or document contingency plans in the event of a potential loss of data processing. As a result, CSC is vulnerable to a disruption of service should IT capabilities be rendered inoperable for an extended period of time.

Contingency planning is an essential part of continuing an agency's business operations. By not having a business continuity plan, CSC risks not being able to support its clients if connections to ITD's network were lost. Since ITD maintains the network that supports CSC's application, the business continuity planning process should include instructions on how to coordinate with ITD if network connectivity were interrupted. Significant delays can occur by users not being able to access the network in a reasonable timeframe, thus causing backups in the input of key data information onto CSC's network application.

The core of the business continuity planning process involves a commitment from management. Senior management should be involved in the business continuity process so that there is an understanding of CSC's information system environment. Although not formally documented in a business continuity plan, there is emergency contact information listed for CSC employees in the agency's Internal Procedures Handbook. The handbook also states that in the event of an emergency, where there is no access to One Ashburton Place, Boston, hearings could be held in the State Office Building located in Springfield as well as a second location at the University of Massachusetts Dartmouth School of Law. However, there are no formal written plans to obtain applications and continue data processing.

Although CSC's mission-critical application is backed up off-site by ITD, which is under the governance of the Executive Office of Administration and Finance (EOAF), CSC does not have an official written agreement in place with ITD to obtain its mission-critical application, or actions to be taken by ITD to restore the application used by CSC in the event of a business interruption. An effective business continuity plan should provide instructions for different courses of action to be taken for different kinds of disaster scenarios. Moreover, the plan should specify the ways essential

services would be provided without the agency's data processing facility. The plan should also identify the procedures to be followed that detail the logical order for restoring key data processing functions for the original site or at the alternate site. Generally accepted business practices and industry standards for computer operations recommend the need for CSC to have an ongoing business continuity planning process that can document access to systems on which it depends for processing or operational needs.

State agencies have been required to perform and document their planning efforts for the continuity of operations and government per executive orders. Between 1978 and 2007, Governors Dukakis, Romney, and Patrick issued three separate executive orders requiring agencies of the Commonwealth to develop plans for the continuation of government services. In 1978, Executive Order No. 144 mandated that the head of each agency within the Commonwealth "make appropriate plans for the protection of its personnel, equipment and supplies (including records and documents) against the effects of enemy attack or natural disaster, and for maintaining or providing services appropriate to the agency which may be required on an emergency basis." In 2007, Executive Order No. 475 mandated "Each agency within the executive department shall conduct activities on a quarterly basis that support the implementation of its Continuity of Government and Continuity of Operations plan and shall submit a quarterly report…" and "Each secretariat within the executive department shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice… Continuity of Operations plan." In September 2007, Executive Order No. 490 mandated "Whereas, to achieve a maximum state of readiness, these plans should be incorporated into the daily operations of every secretariat and agency in the executive department, and should be reviewed on a regular basis and, with respect to agencies supplying services critical in times of emergency, exercised regularly. In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security."

Recommendation

CSC should work with ITD and EOAF to develop a comprehensive business continuity plan that would ensure that CSC is able to access its mission-critical application in the event of disaster. The plan should include instructions necessary for recovery of business operations at an alternate site. We recommend that the business continuity plan be formally reviewed, tested to the degree possible, and approved. CSC should ensure that the plan is reviewed periodically, or upon major changes to

CSC's IT resources or operating environment. Should changes be required to the plan, they should be formally reviewed and approved, and tested to the degree possible.

The business continuity plans should include detailed staff instructions to cover various disaster and recovery scenarios. CSC has documented some disaster recovery steps in its internal control and procedures manual since it has designated an alternate location to continue processing; however, CSC does not have a documented business continuity plan with detailed instructions for staff to ensure recovery of business operations in the event of an unforeseen interruption. The plan should include contingencies regarding staff, equipment, computers, or other resources for the alternate processing site. We recommend that responsibilities be clearly identified and that contact information be specified for all CSC employees, contact personnel at an alternate site, the ITD, EOAF, and vendors. The plan should identify the overall disaster recovery strategy to be executed by ITD and EOAF to assist CSC in regaining business operations. The plan should also identify specific IT-related processes or procedures that CSC staff need to perform, if any. Understandably, recovery of business operations and access to IT capabilities will require a coordinated effort on the part of CSC, ITD, and EOAF.

Although CSC's mission-critical application is backed up off-site by ITD, which is under the governance of EOAF, CSC does not have an official written agreement in place with ITD to obtain its mission-critical application, or actions to be taken by ITD to restore the application used by CSC in the event of a business interruption.

We further recommend that Executive Orders Number 144, 475, and 490 be followed regarding the creation, documentation, maintenance, and training required for a continuity of government and continuity of operations plan.

Auditee's Response

> *We concur that our Internal Controls and Procedures Manual contains emergency contact information for CSC employees and references two alternative locations for conducting hearings (UMASS Dartmouth School of Law; Springfield State Building) in the event that there is no access to our offices at One Ashburton Place.*
>
> *The Commission acknowledges, however, that there is no written formalized business continuity plan regarding computer operations that currently exists. We will work with ANF's centralized IT division to develop a business continuity plan that would ensure that CSC staff are able to access mission-critical applications in the event of a disaster and will incorporate language into our Internal Controls and Procedures Manual to ensure that the plan is updated periodically.*

[CSC agrees with] the recommendation to formalize an agreement with ITD regarding its obligation to back-up and restore our mission-critical case tracking system and allow access to this system in the event of an unforeseen interruption. Upon receipt of the draft report, a request was submitted to ANF's centralized IT division to facilitate such an agreement which will be included as an attachment to the Commission's Internal Controls and Procedures Manual.