The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2009-0863-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AND FINANCIAL RELATED ACTIVITIES AT GLAVIN REGIONAL CENTER

July 1, 2007 through June 30, 2009

OFFICIAL AUDIT REPORT

FEBRUARY 22, 2010

TABLE OF CONTENTS

INTRODUCTION

The Department of Developmental Services (DDS) is organized under Chapter 19B, Sections 1 to 18, of the Massachusetts General Laws and is placed within the purview of the Executive Office of Health and Human Services (EOHHS). The DDS is comprised of 24 area offices that operate within four regions located throughout the Commonwealth – Central/Western, Northeast, Metro, and Southeast. In addition to the area offices, there are six facilities that house developmentally disabled residents and provide outpatient services. The Glavin Regional Center (GRC) is part of DDS's Central/Western Region.

DDS's primary mission is to provide a variety of services, such as residential services, employment assistance, support for families to care for family members at home, transportation, treatment, monitoring, and care to developmentally disabled citizens. During fiscal year 2009, DDS assisted approximately 33,000 clients through various state-operated programs and contracted services with 220 private providers. In conjunction with community-based programs, DDS serves approximately 900 clients in six developmental centers, such as the Monson Developmental Center, Hogan Regional Center, and the GRC, which functions as an intermediate care facility (ICF) that supports individuals within DDS's various regions.

DDS's Central/West Region includes 183 cities and towns in Berkshire, Franklin, Hampshire, Hampden, and Worcester counties. The Central/West Region provides services to 9,353 clients out of eight area offices located in Pittsfield, Northampton, Holyoke, Fitchburg, Southbridge, Worcester, Springfield, and Milford. The headquarters for the Central/West Region is located on the grounds of the Monson Developmental Center in Palmer, Massachusetts. The regional office is responsible for the business-related functions of the GRC facility and community-based programs in the cities and towns located within the Central/West Region.

The GRC is comprised of eight buildings located in Shrewsbury, Massachusetts on 123 acres of land. The Center provides training and support 24 hours-a-day, 7 days-a-week to 52 live-in residents and provides community residents with various day services including short-term evaluation and treatment. GRC has a 12-bed acute-care medical unit where diagnostic evaluation, chronic illness reassessment, and/or psychiatric behavioral intervention may be provided. GRC also has responsibility for four state-operated homes that provide support to individuals with developmental disabilities. Three of the homes are in Shrewsbury while the fourth is located in Gardner, Massachusetts.

At the time of our audit, the GRC employed 220 full-time equivalent (FTE) departmental staff. The staff included 130 FTE employees in support of resident services, 53 FTE staff associated with state-operated community homes located in Shrewsbury and Gardner, 21 nursing department employees, and 16

employees associated with various administrative and maintenance functions. In addition, there were seven FTE University of Massachusetts staff assigned to the Central/Western Region to ensure that revenue is received for services rendered to the GRC facility residents who receive case management and other community services.

The GRC computer operations were configured in a local area network (LAN) and supported by one file server and 84 desktop workstations. The GRC workstations were connected to a Dell PowerEdge file server that is connected by a dedicated leased line to DDS's file servers located in Boston. The GRC file server, which is located in the administrative building, connects through DDS's file servers to the Commonwealth's statewide area network (WAN) to provide access to the Information Technology Division's (ITD) mainframes and file servers installed at the Massachusetts Information Technology Center (MITC). The WAN provides access to the Human Resource Compensation Management System (HR/CMS), Massachusetts Management Accounting and Reporting System (MMARS), and to other mission-critical applications, including Meditech and the Home and Community Services Information System (HCSIS) installed at MITC.

The Meditech system collects personally identifiable and health-related information on all GRC inpatients and outpatients receiving services; HCSIS is an online incident reporting and tracking tool that allows GRC and provider organizations to file clinical information and reports on incidents, investigations, medication issues, and restraint utilizations. GRC also uses a computerized Work Center Payroll Software System to generate and account for resident wages. A dual system of Microsoft Access combined with Internet banking is also used to account for a resident's funds. An Excel-based spreadsheet is used to account for those items where data fields do not exist on the Work Center Payroll Software System and/or the Microsoft Access software.

With respect to network functions at GRC, an EOHHS Site Manager and Network Engineer are responsible for managing data files residing on the file server and for generating backup copies of programs and data files onto magnetic media. EOHHS and DDS are also responsible for the management of the file servers, associated networks, and workstations located at the regional centers.

The Office of the State Auditor's examination focused on an evaluation of IT-related general controls over GRC's IT environment and financial-related activities.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) audit at Glavin Regional Center (GRC) for the period covering July 1, 2007 through June 30, 2009. The audit was conducted from December 15, 2008 to July 24, 2009. Our audit scope included an examination of IT-related general controls pertaining to IT organization and management, logical access security, inventory control over computer equipment, disaster recovery and business continuity planning, on-site and off-site storage of backup copies of magnetic media, authorized usage of agency credit cards, and internal controls to ensure proper accounting and authorized use of Work Center Payroll and Consumer, Café, and Special Funds. In addition, our scope included a review of GRC's control practices regarding Criminal Offender Record Information (CORI) checks for individuals hired or promoted who may have contact with individuals that are developmentally disabled. We also examined GRC's controls over Personally Identifiable Information (PII) and its efforts to comply with the Commonwealth's data breach notification requirements.

Audit Objectives

Our primary audit objective was to determine whether GRC's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be achieved to support GRC's business functions. The audit included an assessment of the adequacy and effectiveness of controls in place to protect the integrity and confidentiality of data and client information contained within the Meditech and HCSIS application systems.

Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities for DDS IT staff supporting GRC were clearly defined, points of accountability were established, appropriate organizational controls were in place and in effect, and whether IT-related policies and procedures adequately addressed the areas under our review. We sought to determine whether a planning process was in place from which strategic and tactical plans would be developed to help direct the use of information technology to fulfill the GRC's mission and goals.

Our objective regarding logical access security was to determine whether DDS and GRC had adequate controls in effect to provide reasonable assurance that only authorized users were granted access to the application systems used by GRC and whether password administration was actively being monitored.

We also sought to determine whether Meditech and HCSIS systems data was sufficiently protected against unauthorized disclosure, modification, or deletion.

Our evaluation of inventory control over IT resources was to determine whether adequate control practices were in place and in effect to accurately account for computer equipment. In addition, we sought to determine whether an annual physical inventory and reconciliation was conducted, and whether DDS and GRC met Chapter 647 reporting requirements regarding lost or stolen computer equipment. We also sought to determine whether contractual computer equipment purchases were included in the inventory system of record.

With respect to the availability of DDS computing system capabilities in support of GRC's computer operations, we sought to determine whether disaster recovery and business continuity strategies would provide reasonable assurance that mission-critical and essential IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible. In addition, we sought to determine whether adequate control procedures were in place and in effect for the generation and storage of on-site and off-site backup copies of magnetic media to support system and data recovery objectives.

Our audit objective regarding internal controls over financial resources was to determine whether GRC's Consumer Funds Office had procedures in place to provide for the accurate and complete accounting of Work Center Payroll and Consumer, Café, and Special Funds. Our evaluation of Consumer Funds activities was to determine whether adequate controls were in effect to provide reasonable assurance that resident workers were paid for hours worked, appropriate payroll amounts were deposited to their personal savings accounts, and savings account disbursements were made in compliance with established procedures. We also sought to determine whether controls were in place and in effect to provide reasonable assurance that credit cards issued to GRC staff were used in accordance with policies and procedures for the purchase of gasoline for agency vehicles and retail goods to fulfill resident needs.

Our audit sought to determine whether GRC's procedures were adequate for performing background checks on individuals hired or promoted to positions performing sensitive functions or on individuals accepted into specific programs that involve contact with developmentally disabled individuals. We also sought to evaluate whether there were adequate controls in place to protect Personally Identifiable Information (PII) and to determine whether GRC's control policies and procedures supported compliance with the Commonwealth's data breach notification requirements.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding DDS and GRC's overall mission and IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of activities and the internal control environment, we reviewed DDS and GRC's mission and primary business functions. In order to select areas to be reviewed, we performed a risk analysis of IT operations, selected applications, and financial-related activities. We assessed the strengths and weaknesses of the internal control system for selected IT activities, including organization and management, logical access security, inventory control over computer equipment, business continuity planning, on-site and off-site storage of backup copies of magnetic media, authorized usage of agency credit cards, and internal controls to ensure the proper accounting and authorized use of Consumer, Café, and Special Funds. We also reviewed control practices regarding CORI checks and GRC's efforts to comply with PII standards and the Commonwealth's data breach notification requirements. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure of DDS's IT functions that support GRC's IT operations. For the areas included in our review, we determined whether policies and procedures were documented, approved, and communicated to appropriate staff. We reviewed DDS's strategic and tactical plans as they pertain to GRC's activities and functions and its use of IT Resources. To determine whether IT-related job descriptions and job specifications were up-to-date, we obtained a current list of the personnel employed by the DDS IT Department, and compared the list to the IT Department's organizational chart and IT functions performed. In addition, we reviewed and performed selected preliminary audit tests relevant to documents such as the network configuration, internal control plan, and continuity of operations plan.

To evaluate whether only authorized user access could be gained to the GRC's network and systems, we reviewed DDS's and GRC's logical access security policies and procedures with the responsible security administrators. To determine whether logical access security controls were in place and in effect, we reviewed and evaluated the administration of logon IDs and passwords and selected control practices regarding logical access to network resources. To assess whether all users with active privileges were current employees, we obtained a list of individuals granted access privileges to e-mail accounts and other business-related applications, such as Meditech and HCSIS, and compared all users with active access privileges, as of April 29, 2009, to GRC's list of current employees, including administrative and

outsourced staff. To determine whether access privileges that were no longer required or authorized were disabled in a timely manner, we also compared the active network user listing to GRC's listing of terminated employees and their respective termination dates. Furthermore, we reviewed password configuration and whether all persons authorized to access information system resources were required to periodically change their passwords and, if so, the frequency of the changes.

To determine whether DDS and GRC complied with Commonwealth of Massachusetts regulations for fixed-asset accounting for equipment allocated to GRC, we reviewed evidence supporting DDS's performance of an annual physical inventory and reconciliation to the computer equipment inventory records. To determine whether adequate controls were in place and in effect to properly account for GRC's computer equipment, we reviewed inventory control policies and procedures and requested and obtained DDS's inventory system of record for GRC's computer equipment. We reviewed DDS's inventory system of record dated January 14, 2009 for IT equipment installed at GRC valued at $51,882 to determine whether the inventory contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. We also performed a data analysis on the inventory record of computer equipment to identify any unusual distribution characteristics, duplicate records, or unusual or missing data elements. To determine whether the inventory system of record for computer equipment was current, accurate, complete, and valid, we used Audit Command Language (ACL) software to select a statistical sample of 23 items, with an associated value of $4,580 out of a total population of 233 items. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory record to the actual computer equipment.

To verify the relevance and completeness of GRC's system of record for computer equipment, we selected 22 additional computer hardware items in adjacent locations to our original inventory sample and determined whether they were properly recorded on GRC's inventory record. To determine whether all GRC computer hardware purchases in fiscal years 2008 and 2009 were accurately listed, we selected four invoices consisting of six items valued at $5,230 and verified whether the amounts recorded on GRC's purchase orders and related vendor invoices were properly recorded on the inventory system of record.

To determine whether DDS and GRC complied with Commonwealth of Massachusetts regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT equipment disposed of during the audit period, as well as IT equipment that GRC planned to request Commonwealth approval to dispose of as surplus. Finally, to determine whether DDS and GRC were in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we reviewed incident reports for missing or

stolen IT equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the level of planning and the procedures to be followed to resume computer operations in the event that computing system capabilities become inoperable or inaccessible. We interviewed DDS and GRC management to determine whether the criticality of application systems had been assessed, whether an IT risk analysis for computer operations had been performed, and whether a Continuity of Operations Plan (COOP), disaster recovery plan (DRP), and business continuity plan (BCP) were in place and, if so, whether they had been adequately tested. In addition, we reviewed the status of management's efforts to designate an alternate processing site to be used in case of an extended disruption of computing system availability.

We interviewed the DDS Operations Manager responsible for the daily/weekly electronic backup of all applications and associated data files utilized by GRC and reviewed the current backup procedures in place for their adequacy and completeness, including those in place for the mission-critical Meditech and HCSIS systems. Furthermore, we interviewed responsible personnel to determine whether they were formally trained in the procedures of performing media backups and were aware of the procedures for the off-site storage of magnetic media, and the steps required ensuring the restoration, protection, and safety of the backup magnetic media.

Our review and analysis of Consumer Funds Office activities was to determine whether resident funds were accounted for in compliance with GRC policies and procedures and Department of Developmental Services 115 Code of Massachusetts Regulations (CMR) 3.08 - Funds Belonging to Residents. To verify that resident worker payroll documentation conforms to existing procedures, we reviewed and analyzed personal bank account statements, weekly pay sheets, production worksheets, and worker performance records. To ensure appropriate payroll amounts were deposited to the resident's personal savings accounts, we analyzed and compared policies and procedures to the Work Center Payroll distribution spreadsheets, GRC calculation spreadsheets, Access database transaction sheets, TD Bank ACH reports, and TD Bank deposit slips. Furthermore, to determine that GRC was in compliance with existing procedures and regulations regarding withdrawals from resident's personal savings accounts, we evaluated documentation that included an analysis of transfer to disbursements, grouped transactions, and TD Bank WebExpress Community. Lastly, to verify that credit card transactions for purchase of gasoline and retail goods and services were in compliance with internal controls, we compared automobile mileage records and retail credit card receipts to their respective monthly statements and purchase orders.

We interviewed senior management and reviewed GRC's procedures and control practices to determine whether Criminal Offender Record Information (CORI) checks were performed prior to employment or for a change in position responsibility for individuals who would have unsupervised contact with developmentally disabled individuals. To assess effectiveness and compliance with GRC's policies and procedures pertaining to mandatory background checks, we reviewed 53 out of the total population of 238 GRC employee personnel files and tested related documentation. We reviewed Chapter 6, Sections 167-178B, and Chapter 6, Section 178C-178P, of the General Laws and Executive Office of Health and Human Services 101 Code of Massachusetts Regulations (CMR) 15.00-15.16 Criminal Offender Record Checks. We compared required information outlined within 803 CMR 3.05 Sections 1 and 2 with GRC's CORI Request Form to our statistical sample of employees.

To determine the status of GRC's compliance with respect to the handling of Personally Identifiable Information (PII), we reviewed Chapter 93H of the Massachusetts General Laws and Executive Order 504 to identify agency responsibilities regarding protection of PII and notification for confidentiality breaches. We interviewed senior management and completed a PII assessment questionnaire regarding the protection of personal information of GRC's clients and staff.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Criteria used in the audit included Chapter 93H of the Massachusetts 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.

AUDIT CONCLUSION

Our audit of the Glavin Regional Center (GRC) found that internal controls were in place to provide reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, on-site and off-site storage of backup copies of magnetic media, administration of the Special Funds account, and protection of personally identifiable information (PII). However, controls needed to be implemented or enhanced to provide reasonable assurance that logical access security is limited to only authorized users and a comprehensive business continuity strategy and disaster recovery plan is in place to ensure that information system capabilities could be regained within an acceptable period of time. Although we found that policies and procedures were in place to protect financial resources, we determined that GRC needed to strengthen controls to ensure the accuracy of documentation associated with use of agency credit cards issued to GRC staff as well as the recording and approval of Consumer Funds and Café Funds. In addition, we found that GRC needed to enhance controls to effectively monitor and evaluate whether Criminal Offender Record Information (CORI) background checks were consistently performed prior to an individual's employment. We also found inventory controls over computer equipment were adequate except for the absence of certain data fields pertaining to acquisition date, cost, and the name of the individuals to whom the equipment was assigned.

Our review of IT management and control indicated that the Department of Developmental Services (DDS), which supports GRC's IT functions, had an appropriate and defined organizational structure and chain of command for the IT Department with assigned reporting responsibilities and documented job descriptions. DDS also had documented IT strategic priorities that addressed GRC's IT environment and the mission-critical Meditech and the Home and Community Services Information System (HCSIS) applications. Regarding internal control documentation, GRC has an Internal Control Plan (ICP) to assist management and staff in working in conjunction with DDS to ensure that appropriate controls are implemented and exercised to achieve operational objectives and avoid undesired events, such as overspending, operational failures, and violations of law.

Regarding logical access security, our audit revealed that DDS and GRC needed to strengthen controls over network resources to ensure that only authorized users have access to application systems and data files. We determined that in addition to logging onto the network, a user must also enter a unique user ID and password to logon to GRC's mission-critical Meditech and HCSIS applications. Although DDS and GRC had documented procedures in place for the authorization and activation of user IDs and passwords for the network and Meditech and HCSIS applications, controls needed to be strengthened to ensure that user accounts would be deactivated in a timely manner when user access is no longer

authorized. We found from our test of active user accounts to the current payroll that controls needed to be strengthened to ensure that GRC immediately notifies DDS to disable network, Meditech, and HCSIS access privileges for staff that are no longer employed by GRC. We determined that although password rules were in place to allow for acceptable logon security to the network and HCSIS, we found that the minimum password requirement to logon to Meditech was three characters, which is not in compliance with DDS Executive Office of Health and Human Services Security Standards and Procedures, dated October 2000, that require a minimum password length of eight characters. In addition, we found that GRC needed to update its new employee Policy/Procedures Checklist to include GRC's "Internet Acceptable Use Policy" and Email Policy."

Our audit of inventory controls over computer equipment installed at GRC disclosed that inventory policies and procedures were in place to accurately account for and safeguard IT-related resources. We determined that the data fields of information in the inventory system of record were adequately detailed to identify, locate, and account for all pieces of equipment. However, our examination of the IT inventory system of record maintained by DDS indicated that the usefulness of inventory information and the level of integrity could be enhanced with the addition of certain data fields of information that include acquisition date, cost, and the name of the individuals to whom the equipment was assigned. We tested by inspection the existence and the recorded location of our statistical sample of 23 items consisting of desktops, monitors, and printers with an associated value of $4,580 out of a total population of 233 computer-related items valued at $51,882. Furthermore, to verify the integrity and completeness of the inventory system of record, we judgmentally selected 22 additional IT-related items in adjacent locations to the items selected in our statistical sample. We determined that 100% of the computer-related items sampled were properly identified on GRC's listing of inventory computer equipment. We also determined from our testing that GRC was 100% compliant with respect to controls regarding the purchasing, receiving, and recording of newly acquired computer equipment. Lastly, we found that GRC was in compliance with policies and procedures for the reporting of surplus property to the Operational Services Division and the communication of Chapter 647 documentation concerning missing or stolen items to the Office of the State Auditor.

Our review of business continuity planning indicated that although GRC did not have a comprehensive business continuity strategy, a Continuity of Operation Plan (COOP), dated September 25, 2008, was in place, as well as other documented control practices requiring an alternate relocation site for clients and emergency notification plans. With respect to disaster recovery planning for computer operations, we found that DDS has responsibility for IT equipment and applications installed at GRC. Our audit disclosed that DDS did not have an approved, comprehensive, and tested disaster recovery plan (DRP) to restore computer operations at GRC in the event of a natural, manmade, or technological disaster. We

found that existing plans did not provide sufficient disaster recovery strategies to regain computer operations in a timely manner should a catastrophic event render IT systems inoperable. We determined that due to IT consolidation at the secretariat level, DDS no longer has the option of using the Wrentham location as an alternate IT processing site. To strengthen controls, an updated detailed business risk analysis and impact analysis need to be performed to provide input for completing comprehensive and tested disaster recovery and user area plans that operate in conjunction with GRC's COOP. With regard to backup of magnetic media, we found that DDS transitioned GRC to Active Directory enabling DDS to conduct the electronic daily/weekly backup of network data. In addition, we found that weekly/monthly back-ups of data associated with GRC's mission-critical Meditech and HCSIS systems are stored at the Massachusetts Information Technology Center (MITC) located in Chelsea.

With respect to our review of agency credit cards, we determined that GRC needed to protect against the potential misuse of credit card activity by strengthening controls associated with the monitoring and tracking of gasoline credit card purchases and implementing procedures to ensure that purchase orders associated with retail credit cards are complete and receive appropriate approvals. Based on our reconciliation of gasoline credit card receipts to charges billed by vendors approved by the Operational Services Division, we found that GRC conducted due diligence in ensuring that payments were consistent with existing policies and procedures. However, we determined from our analysis of gasoline credit card activity that there were inconsistencies associated with the date/time of the transactions, odometer readings, and actual vehicle miles per gallon (MPG) when compared to the vehicle's estimated MPG. With regard to retail credit card activity, we determined from our test sample of 21 purchase orders to the credit card sign-in/out log, that GRC was 100% compliant by ensuring that staff signed the log consistent with credit card policies and procedures. Our examination of payment documentation confirmed that 100% of our test sample had a valid receipt that matched the amount on the invoice and reconciled to the invoiced amount to the amount remitted to the vendor. Although GRC ensured that a purchase order was issued prior to release of a credit card, we determined that GRC needed to improve procedures to verify that purchase orders are complete, approved by the appropriate signatory, and are properly recorded in GRC's receiving database application.

Our review of internal controls over financial resources disclosed that GRC needed to improve procedures associated with resident Work Center Payroll (WCP) and certain Consumer Funds activities that involve processing of funds available to clients who reside at the facility. We found GRC's Internal Control Plan, updated as of December 9, 2008, included policies and procedures to administer the WCP and properly account for Consumer, Café, and Specials Funds. We determined that to mitigate the risk of misuse of funds from the aforementioned accounts, GRC has controls in place for segregation of duties and the reconciliation of resident bank accounts. In addition, we determined from our testing that GRC

accurately accounted for funds deposited and withdrawn from the Special Fund account. However, with regard to WCP, we found that GRC needed to improve payroll record retention policies for hours worked, strengthen controls to ensure individual production worksheets are approved by an authorized individual, and verify that the appropriate job code is assigned for hours worked. In addition, we determined that controls needed to be enhanced to verify that resident fund request forms relating to Consumer and Café Funds are complete and approved by authorized individuals.

With regard to background checks, we determined GRC was inconsistent in the manner in which it performed Criminal Offender Record Information (CORI) investigations prior to 1990 at which time the CORI process was centralized at the Central/West Regional office located in Monson. Our audit confirmed that although GRC improved controls with regard to performing CORI investigations subsequent to the centralization of background checks, GRC needed to evaluate and ensure that a CORI check is performed for all current and temporary employees that have potential contact with vulnerable populations. Although we found that CORI report confirmations that indicate "no record" of a criminal finding are stored in a file room that is secured in the evening, we determined the file room is unlocked and unattended during regular business hours.

We determined from our analysis of security controls that GRC has taken appropriate action to protect personally identifiable information from unauthorized disclosure that could potentially be used to uniquely identify, contact, or locate an employee or resident. We found that GRC has provided reasonable assurance that it is complying with the guidelines set forth in Chapter 93H of the Massachusetts General Laws, Executive Order 504 (EO 504), and the Health Insurance Portability and Accountability Act (HIPAA). We noted that a unique user ID and password is required to gain access to GRC's mission-critical Meditech and Home and Community Services Information System (HCSIS) applications. We found that GRC has security controls in place to protect against unauthorized access to electronic Personal Health Information (ePHI). We determined that personally identifiable information is available internally to authorized users on a need-to-know and need-to-perform basis for data entry and/or read-only functions. Through our observations at GRC, we verified that PII-related documents are shredded prior to disposal, offices and file cabinets were locked when not attended, the fax and printer room were secured, and signs were posted throughout the building reminding people to protect personal information. We also determined that transferred or new-hire employees must acknowledge by signature that they have reviewed and understand the Executive Office of Health and Human Services' (EOHHS) Code of Conduct, HIPAA, and EO 504.

AUDIT RESULTS

1. Logical Access Security

Our audit of Glavin Regional Center (GRC) revealed that although certain access security controls were in place, logical access security controls for GRC's information system resources needed to be strengthened to ensure that only authorized users have access to the network, certain application systems, and data files. We determined that in addition to logging onto the network, a user must also enter a unique user ID and password to logon to GRC's mission-critical Meditech and HCSIS applications. We found that DDS and GRC had documented procedures in place for the activation of network, Meditech, and HCSIS user IDs and passwords. Although adequate policies and procedures were being followed to authorize and activate user privileges for access to GRC's network resources, we found that network user accounts were not being consistently deactivated for staff who were no longer employed by GRC. In addition, we determined that inappropriate password configuration rules were in effect for the Meditech application and that users were not signing individual security policy statements. As a result, we found that GRC needed to enhance controls to help ensure that GRC is not vulnerable to unauthorized access to application systems and data that could place the security and integrity of staff and resident information at risk.

We confirmed that the GRC Administrative Assistant prepares the appropriate forms for new-hire/transfer employees who require access to the Meditech and Home and Community Services Information System (HCSIS) applications. In addition, we determined that system request forms were signed by the user and supervisor, and forwarded to the Department of Developmental Services (DDS) Help Desk with a copy to Human Resources (HR). HR is responsible for initiating the process to establish the Network Logon user IDs and inputs new-hire information into the GRC Personnel Database via Lotus Notes Desktop for electronic transmission to the DDS Help Desk. The DDS Help Desk assesses the user's system needs, assigns a security class, configures an appropriate level of access to the Network and mission-critical systems, and provides the Administrative Assistant and Supervisor with logon protocols. The Administrative Assistant then meets with the user to provide logon instructions to the Network, Meditech, and HCSIS application systems. We found that the Supervisor has the responsibility to initiate the process to disable access to network and mission-critical application for users whose employment is terminated. The Supervisor notifies HR and the Administrative Assistant when an employee will no longer be employed or is transferred to another area or agency. HR populates the DDS Personnel Database with user termination information that is electronically communicated to the DDS Help Desk, which in turn disables the user's Network ID. To disable mission-critical ID's, the Administrative Assistant sends an email notification of termination to the DDS Help Desk.

Concerning GRC network logon user IDs, our audit test indicated that of the 108 active user accounts, eight (7%) were for individuals who were not currently employed by GRC. The eight unidentifiable users included three individuals who appeared on GRC's termination list dating back to June 2008. We found that GRC should enhance controls to ensure timely notification to the DDS Help Desk of changes in employment status, including terminations, extended leaves of absence, or employee transfers.

We obtained computer system access lists for GRC's local network resources and the Meditech and HCSIS applications and compared the data against GRC's payroll listing, dated January 12, 2009. We determined from our testing of 79 Meditech users and 83 HCSIS users, that two (3%) and six (7%) user accounts should have been disabled, respectively. We found that GRC should strengthen its process to ensure that mission-critical user access accounts are modified, deactivated, or removed as soon as an individual's employment status is changed and/or the employee is terminated.

Regarding password administration, we determined that written procedures were in place and in effect to identify, log, and investigate terminal access violations. Although GRC followed best practices for password logon protocols to the network and HCSIS, we determined that the minimum password length to access the Meditech application was three characters with no maximum password age and that users are left to change their passwords on their own schedule. While users are expected to change their passwords, there is no assurance mechanism in place to monitor and evaluate whether passwords are changed. We determined that Meditech password requirements were not in compliance with DDS and ITD guidelines for information security and Internet usage which requires that users should use complex passwords that are at least eight characters long and consist of numbers, letters, and special characters. DDS, in conjunction with GRC, needs to ensure that password protocols for the Meditech application are in compliance with existing policies and procedures.

Concerning new-hire documentation, we determined that employees must sign a Policy/Procedures Checklist wherein they acknowledge that HR has reviewed with them all appropriate policies and that the employees understand that it is their obligation to familiarize themselves with each policy. We found that the checklist made general reference to "Computer Policies" rather than list the "Internet Acceptable Use Policy" and "Email Policy" by name. Best practice dictates that users sign each policy to ensure that they acknowledge their responsibilities and that failure to comply with the policies could result in disciplinary action that could include termination of employment. However, at a minimum, each policy should be individually identified by name on the checklist. In addition, we determined that the Confidentiality & Privacy (HIPAA) new-hire employee document should be updated to reference Executive Order (EO) 504 rather than EO 412. EO 504 revokes EO 412 and sets the policy for Executive Departments of the Commonwealth of Massachusetts to adopt and implement measures reasonably needed to ensure the security, confidentiality, and integrity of personal information.

Generally accepted computer industry standards dictate that IT resources be made available to only approved users and that network and other IT resources be used for only authorized purposes. Logical access security controls are also necessary to mitigate risks associated with technological environments, including various internal and external networks. By not deactivating user accounts for users who are no longer authorized to have access to IT systems, strengthening password complexity, and ensuring that passwords are changed on a frequent enough basis, GRC is vulnerable to unauthorized access to application systems and data. For example, as a result, personally identifiable information contained in the Meditech application could be at risk of a breach of confidentiality allowing for identity theft or fraud against a GRC employee or resident.

Recommendation

We recommend that GRC strengthen controls to provide greater assurance that access privileges to both the network and mission-critical applications are deactivated or modified when an employee is terminated or when there is a change in the employee's status resulting in the user no longer being authorized to access or use IT resources. To ensure that only authorized access privileges are maintained, we recommend that GRC implement procedures delineating a central point of contact be used, either HR or the Administrative Assistant, to notify IT personnel responsible for access security of changes in employment status. Sufficient security controls should be exercised to protect the confidentiality and integrity of important and sensitive data and to limit access to data and system functions to only authorized parties.

We also recommend that DDS modify its Meditech password configuration to eight characters, which is the Information Technology Division's (ITD) information technology standard for the minimum length of a password. We recommend that the Password History parameter should be set for a minimum of 10 passwords remembered. We recommend that the DDS EOHHS Security Standards and Procedures be followed that require that passwords should change every 90 days and that passwords will contain at least eight and no more than 20 characters and contain (when technically feasible) at least one special character and one numeric. In addition, DDS policy states that systems will save a rolling list of the last six passwords used and prohibit their reuse until they have rolled off the list. The ITD pamphlet entitled Guidelines for Information Security and Internet Usage states that users should use complex passwords that are at least eight characters long and consist of numbers, letters, and special characters.

Concerning new-hire documentation, we recommend that GRC amend its Policy/Procedures Checklist by replacing "Computer Policies" with "Internet Acceptable Use Policy" and "Email Policy". In addition, we recommend that the GRC Confidentiality & Privacy new hire employee document should be updated to reference Executive Order 504 rather than Executive Order 412. This will help to ensure that employees are up-to-date on the importance of Executive Order 504's scope of safeguarding the

collection, use, dissemination, storage, retention, and destruction of personal information. Lastly, we recommend GRC periodically review its security measures to ensure compliance with applicable best practices and generally accepted IT security standards.

Auditee's Response

In response to the Logical Access Security, we have reviewed the Meditech password policy and are in agreement that we could enhance a number of the password parameters to bring it up to a higher level of security. We have had a number of discussions with Meditech and there are two major improvements that can be made. The character length of all passwords will be increased to a minimum of eight characters. There will also be a new 90-day expiration period, which will force all users to change their passwords. In our discussions with Meditech we have learned that there are some limitations of what the application can do also. Please note that this is proprietary software that is owned by Meditech and some of the recommendations that we and the State Auditors would like cannot be implemented based on the limitations of the application. These issues include a rolling list of previously used passwords and the system recognizing the use of capitol letters and numbers in a password. We will however update our internal policy and ask all users to use capital letters and numbers in their password.

A new policy will be put into effect at Glavin whereby the local HR office will notify the DDS Help Desk when a staff person has terminated employment with the Department. The Help Desk will then deactivate the network access and password for that individual. A log will be kept in the HR office that notes the terminated staff name and the date that this information was sent to the Help Desk.

Auditor's Reply

We commend GRC for working with Meditech to increase the minimum password length to eight characters and initiate a 90-day expiration period that will force users to change their passwords. Although the Meditech application has limitations to enforce the use of capital letters and numbers in a password, we commend GRC for updating its internal policy requiring users to begin the immediate use of stronger password configuration (capital letters and numbers).

We acknowledge that GRC has taken steps to strengthen access security controls to ensure that access privileges for unauthorized users are deactivated or modified. By strengthening its deactivation procedures and maintaining a log, GRC has reduced the risk of unauthorized access to application systems.

2. Disaster Recovery and Business Continuity Planning

We determined that DDS has responsibility for the support of all equipment and applications installed at GRC. Although we found certain objectives for contingency planning existed, we determined that DDS did not have a comprehensive disaster recovery plan (DRP) in place to provide for the timely restoration of business and computer capability functions should GRC's IT systems be rendered inoperable or

inaccessible. We found that GRC had a Continuity of Operation Plan (COOP), dated September 25, 2008, that focuses on restoring GRC's essential business functions at an alternate relocation site and performing those functions for a minimum of 30 days before returning to normal operations. However, we determined that DDS did not have a formal DRP and user area plans that work in conjunction with GRC's COOP to address a catastrophic event that would deny access to GRC's facility for an extended period of time.

During the period of our audit we determined that, due to IT centralization at the secretariat level, DDS no longer has the option to use the Wrentham location as an alternate IT processing site. Our audit found that the Wrentham location has two servers, a stand-alone generator, uninterrupted power supply, and dedicated telecommunication lines that, with the appropriate approval, could be operational within a three-month period. The elimination of an alternate processing site limits the flexibility of DDS/GRC to restore operability target systems and network capabilities at an alternate location in order to gain access to its mission-critical applications that reside at the Massachusetts Information Technology Center (MITC) located in Chelsea. The absence of formally documented contingency plans to address disaster recovery places at risk DDS's ability to ensure that GRC continues to have access to its mission-critical IT applications at MITC in the event of a natural catastrophe (i.e., tornado, flood, wind damage, hurricane, fire), man-made disaster (i.e., terrorism, blackouts), or technology-based event (i.e. cyber attack).

IT contingency planning fits into a much broader emergency preparedness environment that includes business processes and recovery planning. While management had formally assessed the relative criticality of its Meditech application in 2007 and developed various policies, DDS had not updated or recently tested comprehensive recovery strategies that address various disaster scenarios that could result in seriously degraded or lost IT computing capabilities. In addition, we determined that the HCSIS system has never been adequately tested to ensure that users could successfully recover data in the event of an emergency.

Although DDS understands that IT systems may need to be recovered under disaster scenarios, an appropriate risk analysis methodology was not conducted to identify the relevant threats that could render IT systems inoperable or inaccessible, the likelihood of the threat, and expected frequency of occurrence for each disaster scenario. As a result, if a disaster were to occur rendering IT inoperable or inaccessible, DDS would be unable to provide the foundation and structural framework for managing computer capabilities associated with emergency response and continuity of responsibilities supporting GRC's mission within an acceptable time period.

With regard to backup of magnetic media, we found that since the transition to Active Directory effective May 1, 2009, GRC is able to mitigate the loss of essential information by conducting an electronic daily/weekly backup of GRC network data to DDS's data center located in Boston. The development and implementation of a comprehensive DRP strategy will help ensure that backup copies of systems and data files stored off site can be accessed and used in a secure manner to recover IT operations to support essential business processes.

Recommendation

We recommend that sufficiently detailed disaster recovery plans be developed that incorporate criticality and impact assessments, risk management, recovery plan testing and maintenance, recovery procedures, training, and communication. In addition, a security risk assessment of recovery plans should be completed on an annual basis, or upon major IT changes, to assist in ensuring the applicability and readiness to address current business objectives. To help ensure that GRC reacts optimally in the event of a disaster, the DRP and user area plans should be developed to work in conjunction with GRC's COOP detailing GRC's current mission-critical operations, applications, and supporting IT infrastructure and a risk analysis assessment of various disaster scenarios. The DRP should also address IT recovery under circumstances when access to GRC's facility is denied for an extended period of time. The DRP should be an IT-focused plan that includes restoring information systems operability at an alternate processing site. In this regard, until a viable alternative is developed DDS should seek approval to restore the Wrentham location to operational status in order to ensure continuity of IT operations in the event that DDS/GRC's computer operations are rendered inoperable.

GRC's contingency plans should assign specific staff with roles and responsibilities and present detailed steps for them to follow in recovering essential IT systems and operations. The DRP should also address the telecommunications and security issues that would arise if GRC had to conduct off-site computer operations. In addition, the plans should document vendor protocol for the emergency use of computers suitable for gaining access to GRC's mission-critical applications located at MITC. The plans should be adequately tested to provide reasonable assurance of their viability, periodic training should be conducted for IT and operational staff, and hardcopy and electronic copies of the disaster recovery and agency-specific user area plans should be stored in a secure off-site location.

Auditee's Response

Our Central Office MIS staff has met with the Auditors to discuss Disaster Recovery and how it will work for DDS. The work that has been done to date was discussed in length as well as what the Disaster Recovery Diagram outlines. Although some of the disaster recovery processes need to be tested and documented after the Active Directory changes were made, DDS has a positive plan moving forward.

A document that defines what exactly the Disaster Recovery Diagram outlines in more detail is currently being written by the staff in Central Office and will be forwarded when complete.

As noted in Glavin's COOP plan, should the Glavin Regional Center lose its computer access, plans are in place to relocate those staff that need access to computers to the Wrentham Developmental Center. Workstations are available in the training room at Wrentham and can accommodate the necessary staff from Glavin.

At Glavin, Nursing services (which do not require computers) will continue to be delivered to the residents in this situation. Rather than data entering in Meditech, written notes would be taken and then transferred to automated files once the network is restored.

Key staff have cellular phones and are listed in the Facility's COOP plan. These phones would be used to carry on business should the facility lose its phone system as well as the computer system.

Auditor's Reply

We note that GRC and DDS are aware of the need for a comprehensive disaster recovery plan to ensure that business operations and IT services can be recovered and maintained in the event of catastrophic IT systems failure or loss of processing capabilities. We are pleased that DDS plans to develop a comprehensive disaster recovery plan and that GRC's COOP has provisions to access computers at the Wrentham Developmental Center to serve as an alternate site for employees to access essential systems. GRC and DDS should continue to work together to implement a detailed business continuity strategy that incorporates GRC's COOP and DDS's strategy to recover central systems. We are hopeful that DDS in conjunction with GRC will be able to achieve its timetable for completion of a final disaster recovery plan. It should be noted that until a disaster recovery plan is completed and tested, GRC remains at risk of not being able to recover IT processing capabilities within an acceptable period of time.

3. Credit Card Usage

We determined that GRC needed to improve controls to monitor and track gasoline credit card purchases and modify procedures to ensure that purchase orders associated with retail credit cards contain the required information and receive appropriate approvals. Wright Express is a vendor approved by the Operational Services Division (OSD) and contracted to administer the usage of GRC's gasoline credit cards. Although adequate policies and procedures were being followed to reconcile gasoline credit card receipts to charges billed by Wright Express, we found that controls needed to be strengthened to accurately log the date and time of gasoline purchases, record correct odometer readings, and ensure that gasoline usage is consistent with vehicle miles per gallon (MPG). With regard to use of retail credit cards, we found that GRC had procedures in place to ensure that purchase orders were issued prior to authorizing the usage of credit cards and that staff were 100% compliant in signing GRC's credit card log. However, we found that GRC needed to enhance controls to verify the accuracy and approval of retail

credit card transactions and ensure that the activity is properly recorded in GRC's receiving database application.

Gasoline Credit Cards

Our audit of gasoline credit cards included an on-line report obtained from Wright Express of 532 gasoline purchases for all GRC vehicles for the period September 2008 through June 2009. We determined that gasoline credit cards are safeguarded in a locked office in a secured garage located on GRC's premises. We also determined from our review and analysis of credit card receipts and charges billed by Wright Express that GRC conducted due diligence in ensuring that payments were made in compliance with existing policies and procedures. We verified that all invoices in our test sample of eight (35%) vehicles from a total population of 23 vehicles had an associated credit card receipt that corresponded to the amount on the invoice and the payment disbursed to Wright Express. In those instances where there was a missing receipt, GRC would obtain a copy or receive the appropriate approval to pay the invoice.

Although GRC had certain controls in place, we determined that in order to protect against the potential misuse of credit card activity, GRC needed to enhance procedures to accurately track and record gasoline usage. Our audit revealed the following:

- Based on our tests to determine if GRC employees were accurately reporting odometer readings at the time they purchased gasoline, we determined from our analysis of 532 gasoline purchases that there were 17 gasoline purchases totaling $398 where the driver entered the incorrect odometer reading. We determined that the majority of incorrect odometer readings pertained to situations where the odometer reading was lower than the odometer reading at the time of the preceding purchase; i.e. vehicle S101N's odometer reading on 10/25/08 was 10,712. The subsequent gasoline purchase on 11/08/08 indicated an odometer reading of 10,496.
- We found from our test of 532 gasoline purchases totaling $13,147 that there were a total of 20 (4%) gasoline purchases totaling $421 made between the hours of 10:00 p.m. and 12:58 a.m. We determined that 12 of the 20 gasoline charges totaling $231 were made between the hours of 12:04 a.m. and 12:58 a.m. Gasoline purchases made after 10:00 p.m. could be construed as outside GRC's normal hours of operation.
- Our audit also disclosed that when comparing the dates and amount of gallons purchased to the odometer readings and estimated MPG per vehicle, there were five conflicting gasoline purchases totaling $119. One example from our test sample indicated that on June 8, 2008, vehicle I.D. S293L recorded two gasoline purchases at 6:55 a.m. and 7:35 a.m. of 23 and 22 gallons, respectively. Based on the vehicle's average of 15 MPG, odometer readings, and times of purchases, we determined the vehicle could not have used 23 gallons of gas within the aforementioned period between purchases. Accordingly, the second purchase of 22 gallons is questionable.
- With respect to our test between the MPG based on actual gasoline purchase to the estimated expected average MPG per vehicle, we determined from our analysis of

532 gasoline purchases that there were 16 gasoline purchases totaling $290 where there was a difference of 42% or greater between the MPG based on actual fill-up to the estimated average MPG per vehicle. An example disclosed during our testing indicated that based on actual gasoline purchases, vehicle S140U should get an estimated 27 MPG. On January 5, 2009, records show that for vehicle S140U there was a gasoline purchase of 8.7 gallons of gas after having gone 110 miles. The purchase represents an average of 13 MPG, or 47% of the expected 27 MPG that would be purchased for the number of miles driven.

In summary, we found inconsistencies and potential irregularities in the amount of $1,228, or 9%, of total gasoline purchases during the ten-month period September 2008 through June 2009. We were unable to validate the reasons for discrepancies due to inaccurate recordkeeping of logs including the driver's name and reason for purchase/trip. Inaccurate tracking and recordkeeping could result in the misuse of credit cards for personal gain.

Results	No. of Purchases	Questioned Amounts
Incorrect Odometer Reading:	17	$398
Actual MPG to Average Expected MPG:	16	$290
Conflicting Gas Purchases:	5	$119
Purchases Made After 10 P.M.:	20	$421
Total Questioned	58	$ 1,228
Total Population	532	$13,147
Percent of Total Population	11%	9%

Retail Credit Cards

To determine if GRC's use of retail credit cards was in compliance with internal controls, we conducted an analysis of 21 purchase orders totaling $8,200 associated with retail credit card purchases from a total population of 333 purchase orders for fiscal years 2008 and 2009. Staff requesting a retail credit card must have a properly authorized purchase order signed by the appropriate signatory before the Administration office will release a credit card (maintained within a locked safe). To use a credit card, staff must sign the card out using the GRC Credit Card Log that is maintained by the Administration office. The credit card must be returned to the Administration office within 24 hours. The credit card log notes the date of purchase, the dollar amount of the expenditure, and the name of the individual making the purchase. A copy of the purchase order and receipt(s) is forwarded to the Storekeeper who records the purchased item(s) in the Receiving Database application.

Based on a comparison of our test sample of 21 purchase orders to the Credit Card Sign-In/Out Log, we determined that GRC was 100% compliant by ensuring that a purchase order was issued prior to release of a credit card and that appropriate staff signed the log in compliance with current policies

and procedures. In addition, we found that 100% of our test sample had a receipt attached to the purchase order that matched the amount disbursed to the credit card company. However, we found that GRC needed to strengthen retail credit card procedures by ensuring that staff complete all required data fields contained within the purchase order and verify that the purchase order receives proper approval. We determined that of the 21 purchases orders reviewed during our audit, five purchase orders (24%) totaling $1,427 (based on receipts attached to purchase orders) were approved with no dollar amount specified and one (5%) in the amount of $229 had no authorization signature. We found that dollar amounts on purchase orders for services were sometimes left blank because labor charges were unknown at the time of issuance. Open-ended purchase orders could result in over-spending of budgeted dollars or misuse of retail credit cards.

During our audit, we identified that GRC maintains a Receiving Database application to inventory and track all purchased goods. Based on our analysis of 21 purchase orders in our test sample, we determined that eight items (38%) totaling $2,137 were not recorded in the receiving database application. Items not recorded in the receiving database application could result in incomplete documentation of purchases, potentially increasing the risk of delays in payments to vendors, undervalued inventory, and misuse of resources.

We note that based on our discussions, GRC had improved monitoring controls to better track and record gasoline credit cards and to utilize Wright Express on-line functionality to examine irregularities associated with inconsistencies with vehicle odometer readings and actual versus estimated MPG. We also note that GRC has implemented controls to ensure that purchase orders pertaining to retail credit card purchases contain all required information, receive appropriate approval, and are properly recorded in the receiving database application.

Recommendation

With regard to gasoline credit cards, we recommend that GRC and Wright Express work together to implement controls to not accept credit cards if the mileage input at the time of purchase is lower than the mileage input at the time of the previous purchase. Action should be taken to activate the Wright Express Driver ID field and require drivers to enter their employee ID at the time of gasoline purchase. We also recommend that parameters be set to not accept credit cards after reasonably agreed upon business hours. GRC should monitor Wright Express on-line reports to identify any irregularities including multiple purchases of gasoline for the same vehicle on the same day or when the number of gallons purchased exceeds the estimated amount of the vehicle's MPG. Management should also implement procedures to review vehicle mileage logs to ensure that they accurately reflect the vehicle ID, driver ID, date and time of vehicle use, to and from locations, odometer reading, and purpose of travel.

Concerning retail credit card purchases, we recommend that GRC initiate procedures to withhold issuance of credit cards if purchase orders are not properly completed, do not include the requested amount, and do not have an appropriate approval signatory. In situations where the amount is unknown, GRC should make an effort to have the vendor provide an estimated charge and note the purchase order with a "not-to-exceed" dollar amount. In the event the amount of goods or services is greater than the "not-to-exceed" amount, we recommend that GRC issue an amended purchase order with the appropriate approval. We also recommend that GRC strengthen controls to ensure purchase orders are recorded in the Receiving Database application by implementing procedures to periodically monitor, track, and reconcile the required entries. Consideration should be given towards initiating a purchase order log to include sign-off when the information is entered into the Receiving Database application.

Auditee's Response

RETAIL CREDIT CARDS

Our policies and procedures for the use of retail credit cards have been revised and are noted below. At the suggestion of the Auditors, we will not issue a credit card to a staff person if the Purchase Order is not filled out completely and properly. In that case, the PO will be returned to the staff person in order that all information is completed. Additionally, should the exact amount of the purchase not be known, the notation "not to exceed" with a dollar amount will be listed on the PO. Finally, should the actual purchase price be different from the amount listed on the PO, the new amount must be listed and signed off by an approved signatory.

A copy of the PO is then sent to the Storeroom to be entered in the Receiving Database. A copy of the "receiver" is then attached to the PO and sent to the Business Office.

DEPARTMENT OF MENTAL RETARDATION
REGION 7
FACILITIES MANAGEMENT
GLAVIN REGIONAL CENTER
CREDIT CARD PROCEDURES

I. Introduction

Credit cards for Retail Stores are being assigned to the Glavin Regional Center. The reason for providing the cards at these sites is to make shopping at retail stores easier for the staff. A staff person (and a backup) who would be responsible for the cards must be identified by the Facility

Security

Credit cards are to be held in a secure (locked) location and this location should be checked daily to ensure that the card is in the possession of the office. The Business Office will maintain a master listing of the credit card numbers assigned.

II. Procedures

Cards are not to be given out to staff unless the following conditions are satisfied.

The staff person must have a purchase order properly authorized before the card is given for use. The purchase order must contain a description of the merchandise to be purchased and dollar amount is to be noted. In the event that the exact purchase price is not known, the notation "not to exceed" with a dollar limit must be entered.

When a card is given out to staff, that staff member must sign out the card (sample log attached) and then return it to the office no later than the next business day. Cards are not to be kept over a weekend. Upon returning the card, the amount of the purchase is to be noted on the log and the designated staff person in the Facility would sign off on the log that the card had been returned.

In the event that the purchase price is different than the amount listed on the purchase order, the new amount must be written in and signed off by an appropriate signatory.

A copy of the purchase order is then sent to the Storeroom in order that the purchase can be recorded in the Receiving Database. A copy of the "receiver" is then attached to the Purchase Order and forwarded to the Business Office for payment. The Credit Card log is then sent to the Business Office on a monthly basis in order to reconcile and note any discrepancies.

In the event that any discrepancies are noted by The Business Office, the Facility is to be contacted with the information regarding the discrepancy so that the matter can be researched and reconciled.

Once the matter is reconciled, the Business Office is contacted so that payment can be made.

III. Loss or Theft

In the event that a card is missing, the Central/West Regional Business Office must be notified immediately. The Business Office will contact the store and inform them of the situation.

GASOLINE CREDIT CARDS

Regarding the use of Gasoline Credit Cards, the following procedures have been implemented to enhance the security of gasoline purchases for the vehicles housed at the Glavin Regional Center.

In the event that a gasoline purchase is made outside of the parameters set below, Wright Express will automatically notify us via e-mail of the purchase so that we can immediately address the discrepancy.

The employee ID number must now be used in order to activate the pump to make a gasoline purchase allowing us to identify who made all purchases.

The gasoline purchases are then reviewed on a weekly basis to ensure that the procedures listed below are followed and to reconcile any discrepancies.

A quarterly review will be conducted with representatives from Wright Express to review our procedures and make any adjustments to those procedures in order to strengthen controls.

1. *Wright Express have been contacted and provided a list of current employees at the center along with their unique employee identification number. Wright Express has agreed to update their system by imputing this data so that all future purchases will require the purchaser to use their employee identification number in order to activate the purchase of gasoline.*
2. *The current program does not allow restrictive access outside of business hours however Wright Express will provide immediate e-mail notification for any purchases made that conflict with the parameters set by the Glavin Regional Center. The following are the parameters submitted to Wright Express;*
    - *Purchases outside of the normal business hours of 7:00 AM – 6:00 PM Monday – Friday.*
    - *Multiple purchases any day.*
    - *Inaccurate odometer readings.*
    - *Purchases were the average MPG is below 15 or higher than 30.*
3. *Weekly monitoring of reports will continue by the facility staff. All discrepancies will be addressed immediately.*
4. *A quarterly review of data will be conducted with a representative from Wright Express in order to monitor current parameters and incorporate new parameters if deemed appropriate.*

Auditor's Reply

We are pleased that GRC has taken the appropriate steps to modify its policies and procedures to ensure that adequate controls are in place for the appropriate use and monitoring of both retail and gasoline credit card activity. With regard to gasoline credit cards, we commend GRC for implementing procedures to monitor mileage, ensure that employees enter their ID at the time of gasoline purchase, and track gasoline charges outside normal business hours. GRC's weekly and quarterly monitoring with representatives from Wright Express will also ensure that gasoline is purchased within established guidelines.

With regard to retail credit card purchases, we are pleased that GRC initiated policies and procedures to ensure that purchase orders are properly completed, include the requested amount, and have an appropriate approval signatory. We also commend GRC for implementing a process to ensure that a "not-to-exceed" dollar amount is on the approved purchase order when a specific dollar amount cannot be determined. We also commend GRC for strengthening controls to ensure purchase orders are recorded in the Receiving Database application.

4. **Work Center Payroll and Consumer and Café Funds**

GRC trains its residents to perform work for wages at various businesses within the local community. Wages earned are recorded and deposited to the resident's savings accounts. We determined from our audit of internal controls over financial resources that GRC needed to strengthen policies and procedures concerning GRC's Work Center Payroll (WCP) and Consumer Funds activities associated with the documentation and standard forms used to support the withdrawal of funds from residents' savings accounts. We found that GRC's Internal Control Plan (ICP), updated as of December 9, 2008, included specific guidelines for the processing of resident WCP and the proper accounting of Consumer, Café, and Specials Funds. We also determined from our review of GRC's ICP and organization chart that controls were in place for segregation of duties that included a monthly reconciliation of deposits and withdrawals to/from resident savings accounts and procedures for checks to be prepared by a staff member and signed by the Chief Financial Officer, Budget Director, or authorized designee. Based on our testing, we found no material findings associated with the Special Fund account.

Although GRC had clearly defined procedures for processing the WCP and accurately accounted for the Consumer and Café Funds, we determined that GRC needed to strengthen controls to ensure accuracy in the recording and approval of payroll information monitored on resident time sheets. In addition, GRC needed to implement procedures to provide reasonable assurance that resident funds request forms include the required information on the standard forms and are approved by authorized individuals.

With regard to our review of WCP processes, we determined from comparative testing of resident savings accounts to distribution spreadsheets, GRC calculation spreadsheets, Access database transaction sheets, TD Bank ACH reports, and TD Bank deposit slips that GRC accurately recorded deposits and disbursements in accordance with established procedures. However, based on our analysis of WCP time sheets, we determined that resident work-hours are tracked on daily production worksheets that are discarded after the information is posted to weekly production worksheets. We found that GRC needed to initiate procedures to retain the daily production worksheets in compliance with guidelines as set forth by the Office of State Comptroller's Payroll Retention Policy, updated as of November 1, 2006. Our audit also disclosed that weekly production worksheets are compiled and attached to a transmittal document signed by the supervisors indicating their approval of the enclosed documentation. Sound business practices require that authorized staff sign each worker's Production Worksheet rather than signing a single cover sheet to ensure the accuracy of hours worked.

During our audit, we found that GRC assigns job codes to the hours recorded on the production worksheet to identify the type of work performed and whether time reported was productive or nonproductive. GRC prepares a quarterly summary of the hours designated to each job code and records the information within the Meditech system on each individual's medical record. GRC and the

Department of Public Health review the information to ensure that each worker is functioning within accepted competitive standards for the assigned job and is compensated according to state and federal regulations associated with wages, hours, and work. The information is also used to complete the worker's merit rating form. Based on our comparison of the hours recorded on the production worksheets to those indicated on the computer-generated worker performance record, we determined that although wages were correctly paid, there were instances where job codes were incorrectly assigned to hours worked. Of the 128 production worksheets in our test sample, we determined there were 11 incorrect job codes recorded on 10 production worksheets (8% error rate). GRC needed to enhance controls to provide reasonable assurance that the appropriate job code is accurately reported as "Hours Worked," "Pieces of Production," or "Nonproductive Time." In addition to the potential for the under or over payment of wages, the inaccurate recording of job codes and hours could impact GRC's ability to ensure that workers are functioning within their limitations and compensated accordingly. The discrepancies could also impact the worker's quarterly merit rating which in turn could impact compensation.

We determined from our review of the payroll signatory sheets for each of the seven weeks covered during our test period that each sheet contained an average of 20 resident workers and that there was an average of three workers per sheet that did not acknowledge receipt of their wages by signing in the appropriate place. GRC's ICP indicates that workers must sign the payroll signatory sheet acknowledging receipt of their wages. The ICP also states that when clients cannot sign their name and sign with an "X" or other mark, there must be a countersignature by an agency staff member in order to verify receipt of pay by the individual. The average error rate for the absence of a verifiable signature was 16%. We found GRC needed to implement procedures to ensure that there is a countersignature for those individuals who are unable to sign their names due to diminished capacity or poor motor skills.

Resident fund request forms must be completed with all required information to support the withdrawal of funds from resident's accounts. Based on our testing of funds available to clients who reside at the facility, we found that resident funds request forms received appropriate signature approvals, receipts were attached and matched expenditures, and unexpended funds were deposited to the resident's savings account. However, we determined that controls needed to be strengthened to ensure that resident funds request forms are signed by the recipient of the funds, amounts returned are accurately recorded on the yellow copy, modifications to the original amount requested are initialed by the approver, and requested amounts are not left blank. We found that of the 118 resident funds request forms in our test sample, 27, or 23%, were not in compliance with Consumer Funds policy and procedures as detailed in the following chart:

Category	No. of Items
Amount received not acknowledged on original form	14
Amount returned blank	3
Increase not initialed by approver	6
Original total request blank	4
Total not in compliance	27

We determined that GRC would be unable to resolve discrepancies if the individuals receiving funds do not indicate their acknowledgement by signing the original resident funds request form. Moreover, if the approver does not initial/sign subsequent changes to previously approved amounts or if the money requested field on the resident funds request form is left blank, the potential exists that funds may be used in a manner that was not originally intended by the approver. In summary, insufficient controls may allow for a situation where residents may not benefit from funds withdrawn from their personal savings accounts.

We note that based on input from the audit team, GRC immediately initiated corrective action to improve controls and procedures to ensure accuracy in the processing of Work Center Payroll and resident funds request forms.

Recommendation

We recommend that GRC fully develop and initiate monitoring procedures to retain the daily production worksheets in compliance with guidelines as set forth by the Office of State Comptroller's Payroll Retention Policy. GRC should conduct a feasibility study to determine whether the use of the daily production worksheet can be eliminated and/or combined with the weekly production worksheet. Tracking hours and assigning job codes on one worksheet would eliminate the possibility of any transposition errors and the necessity to retain additional documents.

We recommend that GRC strengthen controls to ensure the accuracy of job codes recorded on production worksheets before they are forwarded to the Consumer Funds Office for processing. We recommend that GRC map job codes and job descriptions to their respective categories referenced on the production worksheets. If possible, the computer-generated worker performance record should be configured to produce an exception report for those job codes that do not fall within the appropriate time card category. We also recommend the elimination of the transmittal document for weekly production worksheets that supervisors sign and instead supervisors should acknowledge that they have reviewed job codes and hours worked by signing each worker's respective production worksheet.

We recommend that GRC strengthen its controls to ensure that all the required signatures on the payroll signatory sheet are obtained in order to acknowledge receipt of wages. In instances where workers are

unable to provide a signature or sign their name with an "X" due to diminished capacity or poor motor skills, we recommend that, in addition to having a work center staff member sign the payroll signatory sheet, he or she should also make note of the reason why a signature on behalf of the worker is necessary. Due to the illegible manner in which some workers sign their name, we also recommend that GRC develop a cover sheet to be attached to each payroll signatory sheet that the Consumer Funds Office should sign to verify that they have obtained all the required signatures. This will help to fulfill GRC's control objective of ensuring that internal procedures are followed to verify that workers receive their wages on the date they are paid.

GRC should improve procedures to ensure that the resident funds request forms have a signature on the original request form to acknowledge receipt of money. In addition, GRC should ensure that amounts returned are noted on the form and that the approver initials modifications of requested amounts. Lastly, we recommend that GRC ensure that the amount requested is not omitted from the form. We recommend that the Consumer Funds Office withhold disbursements if a resident funds request form is incomplete and/or did not contain the appropriate signatures.

Auditee's Response

Due to discrepancies within the preparation and approval of the payroll at the Glavin Regional Center's Work Center brought to our attention by the Office of the State Auditor, the following corrective procedures have been implemented:

Change in Current Piece Rate Payroll system

As of December 27, 2009, a new payroll software system will be implemented by the Consumer Funds Office. The software changeover will require a change from a piece rate payroll system to an hourly rate payroll system. The new payroll software program will allow for increase in accuracy within the payroll processing function including the payroll calculation of four different pay rates for each employee utilizing unlimited job categories for unlimited employees. The conversion of the piece rate system will require a change for the GRC Work Center with job costing and time study analysis while allowing for a more reliable, yet simple procedure for employee timekeeping and payroll payment. The utilization of the new payroll software will also allow for the ease in preparation of federal payroll tax forms and year end processing of employee W-2's which will decrease the overall accounting costs for the GRC Work Center as well as an increasing the availability of valuable payroll processing informational reports.

Daily Production Sheet

The Daily Production Sheets have been revised to encompass a full week's worth of production tracking. All Work Center Vocational Instructors and Habilitation Coordinator have been re-trained in the implementation of this document.

The original Daily Production Sheets will be attached weekly to the Production Work Sheets, which is submitted to the Consumer Funds Office on a weekly basis. Additionally, a photocopy of the Daily Production Sheets will be kept in the Rehabilitation Counselor's office as a permanent back up.

As of December 27, 2009 when the new payroll system will be implemented by the CFO, all Daily Production sheets will be kept in the Rehabilitation Counselor's office. A new Weekly Hourly Summary Sheet detailing employee name and hours worked will be emailed to the Consumer Funds Office for payroll processing. This document must be emailed to the CFO by the Vocational Rehabilitation Counselor or the Program Manager as it will contain their email signature. Any payroll documents emailed from anyone other then the Voc Rehab Counselor or the Program Manager will not be considered approved for processing and will be considered null and void.

Production Number Reference Sheet to be revised

The reference sheets for all the production numbers (paid versus non-paid) will be revised. The revision will clearly distinguish between the "Productive Hours" (paid) and the "Non- Productive Hours" (unpaid).

Clarification to 800 series payroll processing numbers

In order to prevent confusion and errors we will eliminate all 800 series and 900 series piece rates as of December 27, 2009. Beginning December 27, 2009, all consumers will be paid hourly instead of by piece rate. Therefore we will have only a competitive hourly rate, an hourly piece rate, a non-paid hourly rate, an hourly rate to reflect different non-work related pay (meetings, appointments, training and holiday, a.k.a. MATH).

All Vocational Instructors and Habilitation Coordinator will be retrained

-Focus upon the importance and impact of the proper preparation and approval of the Daily Production Sheets and the Production Work Sheets.

-Review and provide corrected written examples of the Daily Production Sheets and the Production Work Sheets.

-Review the impact of errors contained within these documents.

-Training in the new hourly payroll conversion including new payroll time-keeping sheets.

Production Work Sheet and impact on the Internal Control Policies and Procedures

The Glavin Regional Center's Internal Control Policies and Procedures will be updated to include the new procedures for the implementation of the new payroll software system and the implementation of the calculation of payroll on an hourly rate.

Production Work Sheet Signatures

Until December 26, 2009, the Production Work Sheets will be signed on each sheet signifying that the entire package is approved for processing. In addition, the Rehabilitation Counselor will review and sign each individual's Production Work Sheets ensuring that every entry recorded on the worksheet is accurate for processing.

As of December 27, 2009, the Production Work Sheets will be signed on each sheet signifying that the entire package is approved for processing. In addition, the Vocational Rehabilitation Counselor will review and sign each individual's Production Work Sheets ensuring that every entry recorded on the worksheet is accurate for processing. A new cover page will be implemented where the Hours will be taken from the daily Production Work Sheets and transferred to a new one-page hourly cover sheet. That sheet, now referred to as the Weekly Hourly Summary Sheet will detail employee name and hours worked in each job pay category. This sheet will be signed off by the Vocational Rehabilitation Counselor or the Program Manager before being forwarded to

the Consumer Funds Office by email with an email signature for processing. The Consumer Funds Office will use this approved payroll sheet to process the new hourly payroll.

Employee Pay Date

Employee payday will be on Fridays. Where Friday falls on a Holiday the Work Center Program will pay consumers on Thursday, or on another day to ensure proper payment before Friday.

Employee Signatures

Work Center employees will sign the payroll signatory sheet acknowledging receipt of their wages. In cases where a consumer is unable to sign their name or mark an "X" a Vocational Instructor or Rehabilitation Counselor will provide the countersignature.

Changes in the GRC Internal Control Policy

Appropriate changes will be made to the GRC Internal Control Policy to detail changes to the implementation of the new hourly pay rate system. The new policy has been updated and is attached.

_____

Program Manager

_____

Rehabilitation Counselor

Consumer Funds and Café Funds

When the discrepancies were brought to our attention by the State Auditors after the initial finding of such discrepancies, immediate changes were implemented to ensure accuracy within the Funds request Approval process;

-All Resident Funds Requisition Approvers were re-trained as to proper form and the importance of the approval signature and the inclusion of all necessary information.

-The Consumer Funds Office will not process any Resident Funds Requisitions that do not contain adequate and proper approval signatures.

-Resident Funds Request forms will not be processed unless all required information is present on the approved form.

-The Consumer Funds Office will not accept any funds requisition forms that have been changed where those changes do not reflect either a new Approver signature or the inclusion of the Approval signature's initials to changes made on the original funds requisition.

-In the above cases all improperly filled out Resident Funds requisitions will be returned to the Approver in order for them to be completed properly.

-The Consumer Funds Office will ensure that all funds disbursed are properly signed for and that all fields within the form are properly filled out in order to record funds returned. All staff associated with this process have been re-trained accordingly.

_____

Director of Consumer Funds

Auditor's Reply

We commend GRC for taking immediate corrective action during our audit to strengthen controls in the areas of Work Center Payroll, Consumer, and Café Funds. We are confident that the Consumer Funds Office purchase of the new payroll software application as well as other procedural changes will help to ensure that adequate controls are in place with regard to all functions associated with the processing of Work Center Payroll and the accounting and tracking of Consumer and Café Fund activities.

We also commend GRC for taking the appropriate steps to modify its policies and standard operating procedures and maintaining a comprehensive and cohesive internal control plan with regard to above-mentioned areas. We recommend that GRC continue to monitor its business processes in order to ensure that internal control policies and practices are kept current to provide reasonable assurance that operational and control objectives will be met.

5. Criminal Offender Record Information

We found that although 115 CMR 11.00 sets forth that a Criminal Offender Record Information (CORI) is required for only those employees who have the potential for unsupervised contact with individuals being provided services by DDS (GRC), our audit revealed that GRC has expanded the requirement to all employees regardless of their positions to include volunteers, interns, students or other persons regularly offering support in either a paid or unpaid capacity. Our audit revealed there was inconsistency in the manner in which GRC performed CORI investigations prior to 1990 at which time the CORI process was centralized at the Central/West Regional office located in Monson. In addition, we found that information from CORI checks where no criminal activity was found was not being maintained in an environment that would ensure security, confidentiality, and integrity.

We determined that prior to centralization of CORI checks, each area within the Central/West Region, including GRC, was responsible for conducting its respective CORI investigations. The process subsequent to 1990 provides that CORI-certified personnel located in the four areas (GRC, Monson, Templeton, and Holyoke Soldiers Home) within the Central/West Region are authorized to order a CORI; however, they do not have the authority to review the reports. The results of the CORI investigations are forwarded to the Central/West Employment Services Manager for review and disposition. We determined from our statistical sample that of the 53 employees tested, nine, or 17 %, did not receive a CORI check. Further analysis indicated of the nine exceptions, eight were hired prior to 1990 and one individual was hired in 2005. GRC procedures and 115 CMR 11.00 indicate that a candidate may not be employed or volunteer service until after they receive clearance as a result of the CORI investigation.

We determined that CORI reports that contain a disqualification for employment due to an unacceptable risk posed by the nature of a crime are stored in a secured file draw in the Employment Services

Manager's office. In addition, we found that the Employment Services Manager complies with 115 CMR 11.00 requirements to notify candidates when their CORI report indicate a criminal finding that makes them ineligible for any position that has the potential for unsupervised contact with persons receiving services. We found that CORI report confirmations that indicate "no record" of a criminal finding are maintained within the employee's personnel file and stored in five-drawer file cabinets in a stand-alone file room located adjacent to the Human Resources department. Although the file room is secured in the evening, the door to the file room is unlocked and unattended during regular business hours. Executive Order 504 requires that executive branch departments of the Commonwealth of Massachusetts adopt and implement maximum feasible measures reasonably needed to ensure the security of personal information. Although the CORI reports stored in the file room do not reveal findings of a criminal nature, other information contained within the employee's personnel files could be available for review by unauthorized individuals.

Our review also disclosed that the GRC new-hire checklist did not reference a check box to indicate that GRC performed a CORI investigation. Utilizing a CORI check box on the new-hire checklist will help to ensure that all necessary CORI documentation is reviewed by all appropriate parties for new hire employees or employees transferring from other agencies.

Recommendation

We recommend that at a minimum, GRC conduct a review of all personnel that have direct unsupervised contact with vulnerable populations and update its CORI investigations accordingly. Particular attention should be given towards those employees hired prior to 1990. Also, GRC should consider implementing controls to periodically update the employee's CORI report every three years on the individual's anniversary date or when they transfer to positions designated as sensitive that may require unsupervised contact with potentially vulnerable individuals. GRC risks not being able to detect unacceptable employee actions when they do not periodically perform CORI background checks on individuals who have direct unsupervised contact with potentially vulnerable groups. We also recommend that GRC take action to secure the room containing the personnel records during regular business hours to ensure that only authorized individuals will have access to personally identifiable information. We note that GRC has initiated corrective action by ensuring that the new-hire checklist used by the Central/West Regional office contains a CORI investigation check box.

Auditee's Response

The Department of Developmental Services appreciates and is in agreement with the State's Auditors suggestion that the Human Resources Offices conduct CORI checks periodically and for those employees before 1990 where evidence was not available that a CORI check was done prior to employment. Before this can happen negotiations must take place with all the unions that represent employees at the Glavin Regional Center

because it is a change in working conditions. In fact, this is an issue that affects not only the Glavin Regional Center but all of the DDS and other human services agencies. Therefore, the negotiations must take place when the collective bargaining agreements are up for renewal. These negotiations are led by the Office of Employee Relations in concert with the agencies.

With respect to securing the files that keep the candidate's CORI checks that do not have a record, the Human Resources Office located on the grounds of the Monson Developmental Center has a system to ensure that this information is held confidentially. The personnel files are kept in a separate room in their office. It has a lockable door to it. Additionally, the main door to the building and the door to the human resources wing where the personnel files are kept also have lockable doors. In fact, the human resources staff are the only ones on campus that have keys to the door that opens that wing where the personnel files are located and the door that opens the personnel file room.

Auditor's Reply

We commend DDS's efforts to work with the Office of Employee Relations to determine if it is permissible to update CORI reports for those employees hired prior to 1990. The actions to be taken should strengthen governance over the process of conducting background checks thereby helping to ensure that appropriate policies are followed and that necessary background checks are performed to protect vulnerable populations.

With regard to the personnel files that contain a candidate's CORI checks that do not have a record, we concur that the information is held confidentially in a separate room that has a lockable door. We also agree that the main door to the building and the door to the human resources wing where the personnel files are kept also have lockable doors and that the human resources staff are the only individuals that have keys to the doors where personnel files are located. We commend DDS for taking appropriate action to ensure the room containing personnel files is kept locked at all times. We recommend that DDS continue to monitor the areas that contain personal identifiable information to ensure that lockable doors are secured and that access is denied to unauthorized individuals.