The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

Boston, MASSACHUSETTS 02108

TEL. (617) 727-6200

No. 2008-0857-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON INFORMATION TECHNOLOGY CONTROLS AT THE CRIMINAL HISTORY SYSTEMS BOARD

July 1, 2006 through October 31, 2008

OFFICIAL AUDIT

REPORT

MAY 5, 2009

TABLE OF CONTENTS

INTRODUCTION

The Criminal History Systems Board (CHSB) was created by Chapter 6, Sections 167 through 178, of the Massachusetts General Laws (MGL) and established within the Executive Office of Public Safety and Security (EOPSS) by MGL Chapter 6A, Section 18. The Secretary of the EOPSS has direct oversight over the Office of the Chief Medical Examiner, Criminal History Systems Board, Sex Offender Registry Board, Department of State Police, Municipal Police Training Committee, Department of Public Safety, Department of Fire Services, Merit Rating Board, Military Division, Massachusetts Emergency Management Agency, Department of Correction, and Parole Board. CHSB is comprised of the Secretary of Public Safety, Attorney General, Chairperson of the Massachusetts Sentencing Commission, Chief Counsel for the Committee for Public Counsel Services, Chairman of the Parole Board, Commissioner of the Department of Correction, Commissioner of Probation and Commissioner of the Department of Youth Services, Colonel of State Police, and nine persons who are appointed by the Governor. The Secretary of Public Safety serves as the Chairman of the CHSB and requested that we conduct this audit. The Executive Director directs strategic planning for CHSB and sets operational priorities for its 61 employees located in its office at 200 Arlington Street in Chelsea. CHSB is supported by a budget of approximately $7.39 million for fiscal year 2009. As of September 2008, there were approximately 3.4 million criminal history files for three million individuals within CHSB's Criminal Justice Information System (CJIS) application.

CHSB's mission is to provide timely and accurate criminal justice information and services to authorized law enforcement and non-criminal justice agencies and individuals in support of promoting the public safety and security of the Commonwealth of Massachusetts. The law requires that CHSB maintain the Commonwealth's criminal justice information system by disseminating Massachusetts Criminal Offender Record Information (CORI), giving assistance to individuals or families who may be crime victims, and maintaining licensing and firearms transaction records. CHSB is organized into five units:

- **Criminal Offender Record Information (CORI) Unit** provides CORI to Board-certified, non-criminal justice agencies such as schools, day care centers, home health care organizations, youth athletic organizations, and municipal government agencies. Individuals may also obtain a copy of their personal criminal record from the CORI Unit. Excluding law enforcement agency requests, the CORI Unit processes an average of 100,000 requests per month. This Unit also assists in correcting inaccurate criminal records, investigates complaints of improper access to or dissemination of CORI, and provides legal assistance on matters relating to the CORI law to police, prosecutors, judges, and the public.

- **CORI Audit, Training, and Compliance Unit** helps ensure that individuals and agencies certified by CHSB to access CORI understand the purposes for which they are authorized to access CORI. The Unit assists individuals and agencies regarding the reading and interpretation of disposition codes and CORI reports; the statutory and regulatory rights of current and prospective employees; the responsibilities of employers with respect to access, review, storage, and dissemination of CORI; consideration of the relevance of a criminal record to the duties and qualifications of various positions; and how to interpret and use the information they receive in a fair and objective manner.
- **Firearms Record Bureau (FRB) Unit** maintains a database of licenses issued including licenses to carry firearms (LTCs), Firearms Identification (FID) cards, gun dealer licenses, and machine gun licenses. The FRB also keeps records of firearms sales by gun dealers, as well as private transfers of weapons. The FRB also answers questions regarding the Commonwealth's gun laws.
- **Victim Services Unit (VSU)** provides assistance to victims of crime. The VSU certifies victims, witnesses, family members of homicide victims, parents and/or guardians of minor-aged victims, and incompetent victims, as well as "citizens in fear," to be notified in advance when an offender is going to be released from prison. The VSU also certifies victims, witnesses, family members of homicide victims, parents and/or guardians of minor-aged victims, and incompetent victims for access to CORI documents regarding the case to which they pertain. Resources, referrals, crisis intervention, and safety planning assistance are also provided as needed.
- **Criminal Justice Information System (CJIS) Support Services Unit** offers law enforcement and criminal justice agencies within the state and across the nation access 24 hours per day, seven days a week to state and interstate criminal history record information, missing and wanted person files, drivers' license and motor vehicle information, and other critical criminal justice information via the National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS).

The CJIS Support Services Unit is comprised of four groups: Technical Services, Application Support, Data Center Operations, and CJIS/NCIC Support. At the time of our audit, the CJIS Support Services Unit consisted of 28 full-time staff members. Each of the four groups has a team site manager under the direct control of the Chief Information Officer, who reports directly to CHSB's Executive Director. CHSB's mission-critical automated system, which is called the Criminal Justice Information System (CJIS), was developed in the early 1980s and is a mainframe-based legacy system. The CJIS Support Services Unit operates and maintains the CJIS application, which is an extensive database containing detailed criminal record information on every convicted adult in the state, which is available to police departments through remote terminals connected to a central network.

CHSB is responsible for the design, security, and management of the Massachusetts statewide CJIS wide area network (WAN). The CJIS network configuration is an Internet Protocol- (IP) based secure private

WAN that provides secure data communications connectivity to a wide variety of local, county, state, and federal law enforcement and criminal justice entities within the Commonwealth. For example, a police department can share its data with another police department over the CJIS WAN.

CHSB is the National Crime Information Center (NCIC) CJIS Systems Agency (CSA) of Massachusetts and also participates in the National Law Enforcement Telecommunications System (NLETS), the Federal Bureau of Investigation's (FBI) Interstate Identification Index (III) program, the Integrated Automated Fingerprint Identification Systems (IAFIS), and interfaces with the Registry of Motor Vehicles ALARS computer network. The CJIS WAN supports over 400 in-state agencies, including local law enforcement, Massachusetts State Police, Department of Correction, Sheriffs, District Attorneys, Department of Youth Services, Parole Board, Department of Probation, Administrative Office of the Trial Court, Registry of Motor Vehicles, and the Merit Rating Board. There are over 25,000 Massachusetts-based users of the current CJIS network. In addition, over 18,000 law enforcement agencies across the country access the Massachusetts CJIS network via NLETS.

The CJIS Network acts as a "hub," serving as the network backbone for the law enforcement community and providing access to in-state and national criminal records, in-state and national wanted person data, in-state and national sex offender registration information, in-state and interstate driving and vehicle records, breath alcohol testing systems, firearms licensing, and other critical public safety information. The CJIS network and data center infrastructure also provides approved public access to certain systems, including the CORI Automated Screen System (CASS), Massachusetts Instant Record Check System (MIRCS), a Massachusetts Military web-based application, the Massachusetts Emergency Management Agency's (MEMA) Electronic Comprehensive Emergency Management Planning (eCEMP) database, and the National Public Sex Offender Registry (NPSOR). The CASS allows for authorized non-criminal justice agency users to electronically submit requests for criminal history information. The NPSOR facilitates nationwide searches across available states' and territories' public sex offender registries from a central location. The CJIS network also connects state agencies, such as the Massachusetts State Police, Sex Offender Registry Board, State Fire Marshal, Parole Board, and the Sheriffs to the Commonwealth's MAGnet network. This connectivity provides access to shared services provided by the Commonwealth's Information Technology Division, including Internet service, the Massachusetts Management Accounting and Reporting System (MMARS), and the Human Resource Compensation Management System (HR/CMS).

We performed an assessment of the functional integrity of CJIS and requirements for upgrading the system in order to ensure the accuracy and completeness of the criminal history records. Our examination also focused on a review of selected internal controls over CJIS, specifically physical security and environmental protection controls over IT resources at CHSB's computer operations and administrative office, system access security, program change control, and on-site and off-site storage of computer-related media. In association with our review of access security we also performed a review regarding the adequacy of controls in place to protect the integrity and confidentiality of personally identifiable information contained in the CJIS database.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, and at the request of the Secretary of the Executive Office of Public Safety and Security, we performed an information technology (IT) general controls examination of IT-related activities at the Criminal History Systems Board (CHSB) for the period July 1, 2006 through October 31, 2008. The audit was conducted from May 2, 2008 through October 31, 2008. Our audit scope included an assessment of the plans in place to upgrade the current Criminal Justice Information System (CJIS). Our audit scope also focused on the functionality of CJIS and determined whether modifications were warranted and resources were available to establish the necessary infrastructure for improving the system in order to ensure the accuracy, completeness, and confidentiality of the criminal history records. Our audit scope also included a general control examination of internal controls related to the organization and management of IT activities and operations, physical security and environmental protection over CHSB's IT infrastructure, program change control, system access security, inventory controls over computer equipment, and on-site and off-site storage of backup magnetic media.

Audit Objectives

Our primary audit objective was to review the current CJIS and to assist CHSB in determining whether its planned upgrade of the system to an integrated enterprise-based system had sufficient merit to meet the operational and business requirements of CHSB. We determined whether adequate controls were in place to provide reasonable assurance that CJIS would be safeguarded and available when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT resources and automated systems.

We determined whether CHSB's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related controls were in place and in effect to support business functions. Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether CHSB had implemented IT strategic and tactical plans to assist CHSB in fulfilling its mission, goals, and objectives and whether CHSB had appointed a steering committee to oversee all IT functions.

We determined whether sufficient environmental protection controls were in place to provide a proper IT environment to prevent and detect damage or loss of IT resources. In addition, we determined whether adequate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources, including the CJIS and other business-related office applications, and that procedures were in place to prevent and detect unauthorized access to automated systems. We also assessed the effectiveness of CHSB change controls over CJIS program files, database software, and operating system software. In addition, we sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment, including notebook computers, was properly recorded and accounted for and safeguarded against unauthorized use, theft, or damage. Lastly, we determined whether adequate procedures for on-site and off-site storage of backup media to support system and data recovery operations were in place.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of CHSB's mission and business objectives. To gain an understanding of the primary business functions that were supported by the automated systems, we conducted pre-audit interviews with the managers and staff and reviewed CHSB's enabling legislation, the Executive Office of Public Safety and Security's (EOPSS) website, and selected documents, such as the "CHSB Integrated Criminal Justice Information System (ICJIS) Project," as of November 2006. Through interviews we gained an understanding of the information technology used to support CHSB's business operations. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. In conjunction with our review of internal controls, we performed a high-level risk analysis of selected components of the IT environment. We developed our audit scope and objectives based on our pre-audit work that included an understanding of CHSB's mission, business objectives, and use of IT technology.

As part of our audit work, we reviewed the organization and management of IT operations that support CHSB's business functions. In that regard, we reviewed relevant IT-related and operational policies and procedures, reporting lines, and IT-related job descriptions. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, policy directives, and generally accepted control objectives for IT operations and security. Regarding our review of IT-related procedures, we interviewed senior management and staff and

completed internal control questionnaires. We reviewed the organizational structure and reporting lines of the CJIS Support Services Unit in order to evaluate span of control, unity of command, assigned functional responsibilities, and points of accountability. To determine whether IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities, we obtained a current list of the personnel employed at CHSB, including their duties and job descriptions, and compared the staff list to the organizational chart and each employee's stated day-to-day IT-related responsibilities. We also obtained and reviewed an IT strategic plan prepared by EOPSS's Integrated Criminal Justice Planning Council that identified existing criminal justice information systems and recommended a strategic roadmap for the future.

We interviewed CHSB management to discuss internal controls regarding physical security and environmental protection over and within the central office, data center, and the on-site storage areas for the backup of magnetic media. We inspected the central office and the data center, reviewed relevant documents, and performed selected preliminary audit tests. To determine whether adequate controls were in effect to prevent and detect unauthorized access to the central office and data center housing automated systems, we inspected physical access controls, such as the presence of security personnel on duty, locked entrance and exit doors, the presence of personnel at the entrance point, intrusion alarms, and whether sign-in/sign-out logs were required for visitors. We reviewed physical access control procedures, such as the lists of staff authorized to access the central office and data center and magnetic keycard management regarding door locks to the central office's entrance and data center. We determined whether CHSB maintained incident report logs to record and identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of computer-related equipment.

To determine whether adequate environmental protection controls were in place to provide proper IT operational environments within which computer equipment and other IT resources are protected against loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply, surge protectors for automated systems, and emergency power generators and lighting installed in the central office and data center. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the data center or in the vicinity of computer-related equipment. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the data center. Furthermore, we checked for the presence of water detection devices within the data center and whether the mainframe, file servers and other computer equipment, and magnetic backup media stored on site were on racks raised above floor-

level to prevent water damage. Audit evidence was obtained through interviews, observation, and review of relevant documentation including equipment maintenance and inspection records.

Regarding the effectiveness of change controls, we reviewed CHSB's policies and procedures for managing program and database changes. We determined which individuals are responsible for applying changes to the operating system and whether the work performed is reviewed by a supervisor on a periodic basis. We also examined and tested the effectiveness of CHSB's controls to ensure that only tested and authorized changes are placed into production for CJIS.

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to the CJIS. CJIS, which resides on CHSB's file servers, is accessed through workstations that are located at CHSB's central office and in-state and out-of-state law enforcement and criminal justice agencies. We reviewed control policies regarding logon ID and password administration and password composition, evaluated the appropriateness of documented policies and guidance provided to CHSB personnel, and interviewed employees from the CJIS Support Services Unit responsible for system access security. In addition, we reviewed control practices used to assign and grant staff access privileges to the application programs and data files. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted to only authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. We determined whether all individuals authorized to access system applications were required to change their passwords periodically and, if so, the frequency of the changes. In addition, we reviewed selected access user privileges, access logs, and evidence that passwords were required to be changed on a pre-determined basis. To verify that all CHSB users of the CJIS application were current employees, we compared a system-generated user account list for CJIS users to a CHSB employee list, dated April 17, 2008. We did not test to verify whether non-CHSB personnel who are certified CJIS users were current employees of their respective agencies.

To assess the adequacy of inventory control procedures for computer equipment, we conducted an examination of CHSB's inventory to determine whether controls were in place and in effect to properly account for and safeguard IT resources. We examined policies and procedures regarding the computer equipment inventory to determine whether CHSB was in compliance with the Office of the State Comptroller's regulations regarding fixed asset control. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of computer equipment. We also performed a data analysis on the inventory and

made note of any distribution characteristics, duplicate records, unusual data elements, and missing values.

To confirm the existence and assess the proper recording of computer equipment, we randomly selected a sample of 71 out of 1,225 IT-related items listed on CHSB's inventory, dated May 8, 2008, to locate the equipment and compare information for identification tag numbers, location, and description to what was recorded. In addition, we selected 46 items of computer equipment from their locations and determined whether the items were properly recorded on the inventory. To determine whether selected computer hardware purchases for fiscal years 2007 and 2008 were accurately listed, we randomly selected 27 computer hardware purchases consisting of 101 items and verified whether the amounts recorded on CHSB's purchase orders and related invoices were accurately recorded on the inventory system of record. We also determined whether any computer equipment had been designated as surplus or disposed of during our audit period.

To determine whether CHSB had appropriate control practices in place and in effect to account for and safeguard notebook computers, we interviewed representatives from the CJIS Support Services. Furthermore, we reviewed the control form regarding CHSB's notebook computer equipment loan policies for employees, and requested for review CHSB's documented policies and procedures to control the assignment and use of notebook computers. We also verified whether all notebook computers listed on CHSB's system of record were locatable.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed the Chief Information Officer (CIO) and staff responsible for the generation and storage of backup copies of data files and software. To determine the adequacy of provisions for on-site storage of backup copies of mission-critical CJIS application and essential magnetic media at the data center, we reviewed physical security over the on-site storage location through observation and interviews with CHSB managers and CJIS Support Services personnel. We did not review Information Technology Division (ITD) backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS).

To determine whether the CJIS application was supporting the mission of CHSB, we reviewed the functionality to assess whether the system was meeting user needs and if application changes were required. We also conducted interviews with a cross section of CJIS employees to gain and record an understanding of the difficulties and deficiencies with the current application system as it relates to their

particular responsibilities. We also reviewed system documentation that included narratives, flowcharts, and record layouts.

Our audit was conducted in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2007. Additional audit criteria included Chapter 93H of the Massachusetts General Laws; Executive Orders 412, 490, and 491; and Chapter 82 of the Acts of 2007.

AUDIT CONCLUSION

Our audit of the Criminal History Systems Board (CHSB) determined that adequate internal control practices were in place and in effect to provide reasonable assurance that control objectives would be met in the areas of IT organization and management, physical security and environmental protection controls, and on-site storage of magnetic media. However, our examination found that controls needed to be strengthened for system access security, inventory control over computer equipment, off-site storage of backup media, and program change controls. Our performance review of the Criminal Justice Information System (CJIS) indicated that the current system is not sufficiently integrated and lacks functionality to meet the needs of the criminal justice community and general public at large. Our review of CJIS revealed errors and missing data in the criminal history records database, reducing the reliability of operational programs that rely on this information. In addition, thousands of criminal fingerprint cards have not been fully processed. Furthermore, CJIS security weaknesses also place the criminal history repository at risk of unauthorized access to the system and data, which could result in sensitive and confidential information being viewed, altered, or destroyed accidentally or deliberately.

Regarding our review of the CJIS application, we found that the system is out-of-date and cannot take advantage of today's technology requiring integration to increase the quality and completeness of data, work efficiency, and ultimately public safety. Moreover, CJIS's older architecture makes it difficult for CHSB to address legislative initiatives, prevents needed database enhancements, increases the difficulty and cost of implementing secure interfaces, and significantly raises the risk of a catastrophic failure of the system. A new enterprise-based public safety and justice information system would provide management with key evaluation and monitoring tools to effectively and efficiently meet business objectives.

Regarding our review of the CJIS application, we found that the system contained inaccurate information and some records were incomplete. The errors, which were caused by data entry and system design problems, can impact the accuracy of background checks for gun purchases and work-related background checks. Currently, there is no established process for the arrest records to be matched with the court's criminal arraignment and disposition system known as the BOP. Moreover, not all individuals who are arraigned from a criminal subpoena are required to be fingerprinted by all courts across the Commonwealth. However, we found that although arraignment information had been entered into the criminal history records database, the fingerprints had not been matched to existing records. In addition, the lack of a link between the arrest data and disposition data could result in reduced accuracy of the information entered into the database.

Regarding our review of controls over the CJIS application data files, we found that controls need to be strengthened with regard to log history for individuals capturing CJIS information by CJIS group users operating through dedicated terminals and the monitoring of CJIS queries being performed on local celebrities. We did find that CHSB support personnel and CJIS system functionality allows for monitoring and adequate security controls for access to CJIS information from mobile law enforcement and virtual private network users. However, we found that CHSB did not have control procedures in place for the authentication of CJIS user groups who have access to the CJIS applications through the legacy mainframe terminals. We also found that CHSB did not have procedures in place to prevent and detect repeated criminal inquiries of local celebrities being made through the electronic CJIS application without an apparent work-related justification.

Our review of information technology- (IT) related organizational and management controls indicated that CHSB had a defined IT organizational structure, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for IT staff that reflected current responsibilities. In addition, our review of IT-related planning found that CHSB had developed comprehensive strategic/tactical plans to address IT functions within the agency. With respect to the use and the safeguarding of information technology, we determined that formal policies and procedures were in existence but needed to be strengthened for off-site storage of backup media and program change control. The absence of sufficiently documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced.

Our examination of physical security revealed that controls provided reasonable assurance that CHSB's IT resources were safeguarded from unauthorized access for the data center and central office. We found that the data center was locked and that a list was maintained of individuals who had key access to the facility. Moreover, CHSB's data center had full-time security guards on duty 24 hours per day, seven days per week, and the facility was equipped with intrusion alarms. Our examination also disclosed that the data center had restricted keycard access to only approved individuals. In addition, visitors were escorted when accessing the data center to minimize the risk of damage and/or theft of computer equipment. Our review of areas housing workstations in the central office disclosed that on-site security personnel make periodic rounds nightly to verify that all office doors are locked and secure.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply, were in place in the building housing CHSB to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were

appropriate. We found that an uninterruptible power system was in place to prevent sudden loss of data and that hand-held fire extinguishers were located within the data center. Moreover, evacuation and emergency procedures were documented and posted within the data center, and, according to management, staff had recently been trained in the use of these emergency procedures.

Regarding system access security, our audit revealed that CHSB had developed and documented appropriate procedures regarding the granting of access privileges for CHSB employees to web-enabled automated systems and activation of logon IDs and passwords. Regarding procedures to deactivate CHSB employee access privileges, we found that formal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. However, adequate password controls, designed to prevent unauthorized access to computer data, have not been implemented for the CJIS legacy application. We found that user IDs and passwords were not assigned in order to gain access to a large selection of data files within the CJIS application, and users were allowed to click on a workstation icon and gain access to many sensitive data files.

Our audit revealed that CHSB could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon, since a complete annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy, completeness, and validity of the inventory record. The absence of a reliable inventory of computer equipment hinders CHSB's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives. Our analysis disclosed that the inventory record did not contain essential information regarding historical cost, date of purchase, installation date, and life cycle status. Our audit test of the inventory record disclosed that of the 71 randomly selected IT assets, 50 items could not be located. Also, we selected 46 items at various locations and found that 24 of these assets were not recorded on the master inventory list. As a result, CHSB could not provide reasonable assurance of the integrity of its inventory system of record for computer equipment.

Our audit also revealed that, contrary to sound business practices, CHSB did not maintain off-site storage for backup tapes for its critical CJIS data files. CHSB management should find a secure off-site location to store its backup computer-related media.

AUDIT RESULTS

1. Criminal Justice Information System

Our review revealed that the mission-critical Criminal Justice Information System (CJIS), which was initially installed over 25 years ago to modernize criminal case records, is not meeting the business needs of Criminal History Systems Board (CHSB) users, the criminal justice community, or the general public at large. CHSB's current CJIS legacy application is out-of-date and cannot take advantage of today's technology to increase data quality and completeness, operational efficiency, and ultimately public safety.

A non-integrated criminal case management system hinders CHSB's ability to fulfill its business objectives, increase inter-agency collaboration, and more importantly, keep current with federal requirements surrounding criminal records history. CJIS's older architecture makes it difficult for CHSB to address legislative initiatives, prevents needed database enhancements, increases the difficulty and cost of implementing secure interfaces, and significantly raises the risk of a catastrophic failure of the system. Additionally, because of the older and proprietary features of this system, support personnel are not readily available in the marketplace, further increasing the cost maintenance and risk of system failure.

Our audit found that the most effective and value-driven solution of whether to modify or replace the current system would be to invest in a new CJIS application and supporting technology. A comprehensive enterprise-based criminal case management system would help substantially by improving the flow of information among criminal justice agencies and creating an environment for sharing critical information at key decision points throughout the justice process.

Our review of the current CJIS application revealed deficiencies in the system's functionality and security. We found that the CJIS application does not have the capability to track criminal record histories on a real-time basis or provide a complete life cycle of a criminal case through its various stages in different agencies without duplication of data collection, data entry, and storage. Our audit also revealed inaccurate information in the criminal history records database, reducing the reliability of public safety decisions that rely on this information. We determined that CHSB was well aware of the operational deficiencies of the CJIS application and had taken appropriate steps to initiate the process of acquiring a new system. However, due to a lack of funds and, possibly, an inadequate focus on continued development of enterprise-based systems within the Commonwealth, a new application system had not been acquired and implemented at the end of our audit.

In the 1980s a "modern" CJIS was purchased by the Commonwealth for the storage and retrieval of criminal history record information, replacing most of the manual recordkeeping by various state

agencies. Today, the CJIS application, operated and maintained by CHSB, is large, difficult, and expensive to maintain. CJIS, which was written in a fourth-generation "COBOL" computer language, requires CHSB to retain or have services to contract programmers specially trained in COBOL. As technology has advanced, COBOL became dated and replaced with more efficient programming languages, limiting the availability of COBOL programmers. In addition, over 25 years of legislative changes required continuous new and complex programming. For example, new laws and penalties for crimes necessitated revisions to a variety of system components. This required an investment of thousands of programming hours and hundreds of thousands of dollars to ensure the CJIS application was capable of receiving, sorting, storing, retrieving, and delivering data as mandated by law.

There have been significant changes in technology since the inception of the CJIS application and supporting technology infrastructures implemented. Unlike other agencies that have been able to upgrade their supporting technology, such as more powerful client servers, CHSB has maintained a less robust functionality for the CJIS application. In March 2006, the Undersecretary of the Executive Office of Public Safety and Security and CHSB management were exploring a similar move, seeking more efficient storage and retrieval of criminal history record data by forming an Integrated Criminal Justice Planning Council. This Council conducted an extensive study of existing criminal justice information systems and recommended a strategic roadmap for the future. This "strategic roadmap" identified the CJIS modernization as a "critical path and essential foundation for the development of the integrated information sharing system."

This new application would replace CJIS with an enterprise-based public safety and justice information system that would provide management with key evaluation and monitoring tools to effectively and efficiently meet business objectives. CHSB management had also indicated through an investment brief in April 2008 to the Commonwealth's Information Technology Division that the new application "provides the foundation to build, deliver, and maintain an effective and efficient enterprise public safety and justice information system by establishing fingerprint-supported records and linking the offender's identity to the criminal history record; improving the accuracy and readability of the criminal record and providing up-to-date dispositions." We also determined that within the new IT Bond Bill IV, CHSB has been allocated a cumulative total of $59 million over a four-year period. The initial outlay of $8.6 million for fiscal year 2009 will be used in order to modernize the existing CJIS application and associated IT infrastructure. However, at the close of our audit, we determined that CHSB had not obtained the initial $8.6 million in first-year funding to develop and implement the new system. Access to the funds has been delayed because of the current fiscal crisis within the Commonwealth. As a result,

the safety and welfare of the public and criminal justice stakeholders continues to be jeopardized until a system is implemented that captures and provides all relevant data related to criminal history records in a timely manner.

Our audit determined that the implementation of a new integrated CJIS application will involve the transfer, or "conversion," of over 25 years of criminal record history data, stored in multiple systems with different syntaxes and formats, into the new system. This conversion of millions of records will be necessary to provide continuity for government agencies that rely on historic case data. The current CJIS application also includes some incorrect data, as the outdated legacy system does not include strong safeguards to ensure that data is accurate and consistent. In redesigning the CJIS application, the goal should be to provide a faster and more user-friendly system for data entry and end users in the field, including patrol officers, prosecuting attorneys, and judges. As crime and homeland security continue to be areas of heightened public safety concern, access to timely and accurate information plays an increasingly important role in all aspects of law enforcement and criminal justice. The information should be available at an agency official's workstation, whether that workstation be a patrol car, a desk, a laptop, or a judge's bench. Users should not have to log into multiple systems or manually compile data from other systems to obtain the information needed to carry out their responsibilities. For example, with a new integrated system, a single request from a user would be capable of retrieving not only traditional Criminal Offender Record Information (CORI)/Board of Probation (BOP) report information, but also the real-time status on an individual including custody status (e.g., incarcerated, under supervision, out on bail), all outstanding warrants, restraining orders, and current conditions of release (e.g., probation, parole, or pre-trial release).

Regarding our review of the CJIS application system deficiencies related to functionality and security, we determined that the current system is unable to reconcile arrests with dispositions, use fingerprints to verify criminal history record information, reconcile all adjudicated court dispositions to specific individuals, and ensure that each individual has only one criminal history record. In addition, the current CJIS application is unable to capture or log event history information that would identify specific users of legacy mainframe terminals who were accessing confidential information or making changes to records without a legitimate work purpose. CHSB employees have also expressed frustration and concern regarding the deficiencies associated with the current CJIS application.

Arrest data is currently being submitted to the State Police Identification System, where it is entered into the State Police Arrest Record System. Disposition data is entered and maintained by the Office of the Commissioner of Probation within the Court Activity Record Information (CARI) central database. We

determined that the CARI central database provides raw criminal history information starting with each arraignment. BOP modifies and distributes the information into a CORI/BOP report, providing information on Massachusetts court appearances that are linked to a Probation Central File (PCF) number that is used to track specific individuals. This data is then made electronically available, through a nightly batch run, to criminal justice agencies through CJIS. However, there is currently no link between the arrest data submitted to the State Police and the disposition data entered by the courts. Without the current system's ability to reconcile arrests with dispositions, CHSB is unable to ensure that that all adjudications are received, recorded, and processed by CJIS in a timely manner in order to accurately and completely reflect each individual's criminal history record.

Our audit revealed that Massachusetts is one of only two states that do not use fingerprints to verify and support criminal history record information. We determined that the BOP report within the current legacy CJIS system is unable to support fingerprints and that users depend upon less reliable methods such as name and date of birth to identify individuals. Not positively identifying individuals using unique information, such as fingerprints, can allow criminal charges to be entered into the system for the wrong person, either unintentionally as an error of data entry or intentionally when the offender gives a false name and birth date. Fingerprinting is considered a "biometric" form of identification that is unique to the individual. Use of biometric identification is an important aspect of a new CJIS system because accurate identification of individuals is key to creating accurate criminal histories. Name, race, and date of birth provide only a partial and sometimes inaccurate identification of the individual. Photographs can help identify individuals, but on their own are also not considered sufficient to establish positive identity. Fingerprints that meet national standards are already stored and available through the state's Automated Fingerprint Identification System (AFIS) and its linked Image Archive System. The system also has the capability to store mug shots using the national standard. Both systems are already linked to the current CJIS and should not pose major problems migrating interfaces to the more advanced and integrated CJIS system of the future.

Our review of the current CJIS application determined that there were significant instances where external CHSB users failed to update certain criminal history records. Our audit tests determined that individuals who were adjudicated of serious criminal acts did not always have their criminal history record updated to accurately reflect these criminal dispositions. Our review revealed 176,869 criminal court cases that were identified within the current CJIS application as arraignments without dispositions. Although the individuals associated with these court cases represent a relatively small number in comparison to the over three million individuals with a criminal history record, our audit was able to identify 38,024 (21%)

that had in fact had their case adjudicated. To get an indication of the types of charges that may remain unmatched, our analysis of this sample indicated that 25% of these court cases had a felony charge ranging from murder to failure to register as a felony sex offender. Of these felony charges, approximately 72% were felony offense seriousness levels "7" through "9," which include rape, rape of a child, kidnapping, manslaughter, and vehicular assault in a reckless manner. The failure to match a disposition with an incident on a CORI/BOP report can mean that criminal histories stored in CJIS are inaccurate and incomplete.

We also determined that CHSB should address problems with the courts, Office of the Commissioner of Probation, and law enforcement that lead to the assignment of multiple probation central file (PCF) numbers to a single offender. The PCF number that is found on a BOP report is used to track individuals. CHSB information is incomplete because some offenders have more than one PCF number. Although each offender in the CJIS system should have one unique PCF, for various reasons dispositions of persons with prior criminal histories do not always match the PCF already on file. For example, an individual may have provided a false name and date of birth upon arraignment, and the criminal record may then be falsely assigned to another person who then appears to have a criminal record. A mistaken identity can also occur when data is being entered into the system and the criminal charge being entered is mistakenly assigned to another person already in the system. The consequence of an offender having more than one PCF is that criminal history inquiries may not report complete information and in some cases causes some CORIs to be incomplete. Our audit tests were able to identify approximately 18,700 manually identified offenders with multiple PCFs. We believe that a larger group of individuals with multiple PCFs would be indicated if more detailed tests of this particular data by criminal justice agencies were completed.

Our audit revealed that there is an ongoing effort through the courts to provide more reliable data to the Commonwealth's CJIS in an electronic mode through the use of the Offense-Based Tracking Number (OBTN) system. This system generates a number, or OBTN, and is assigned by a police department to an arrest record at booking when fingerprints are taken. As a particular criminal event moves through the system, from the police to the courts, each subsequent agency records the number and adds information. The OBTN system helps ensure that all information entered into a criminal record is linked from the original arrest data to the court's disposition data and the individual's fingerprints. Adopting this new system will help address many of the issues raised around mistaken identity and inaccurate report information. The redesign of the new CJIS will make this implementation of automated submission and update more effective by improving the ability to electronically link arrest, disposition, and correctional

data at the individual charge level. The new OBTN could address this issue since fingerprints would be attached to offender records.

We also found that the CJIS application lacked sufficient security controls to ensure that proper authentication for specific users and active monitoring of all users was in place to make certain only authorized and required queries were being performed of criminal history records. According to CHSB management, the age of the application has made it difficult to implement any important program changes, including enhancing security controls of specific users or providing an audit trail to detect any user changes to criminal history records. (See Audit Result No. 2.)

It is important that CJIS reflect complete criminal histories because this database is used by all criminal justice agencies for a wide variety of purposes. For example, detectives use this information when conducting investigations; District Attorneys need complete and accurate histories to make decisions on filing charges, particularly charges related to habitual offenders; Probation officers use criminal histories to develop pre-sentence investigation reports for the courts; and Department of Correction (DOC) staff use criminal histories to determine an inmate's proper identification and custody classification. In addition, complete and accurate data is needed to properly conduct background checks related to gun purchases, childcare and teacher licensing, and employment screening. A disposition on a BOP report makes it less likely that a person will be wrongfully denied or permitted a gun purchase or employment opportunity based on incomplete information.

Recommendation:

We recommend that CHSB management continue to seek approval for funding to support the acquisition and implementation of a new application system to replace CJIS in order to reduce the risk of CHSB's computer systems containing inaccurate or incomplete data. We recommend that CHSB management seek to align use of technology with the mission, responsibilities, and goals of CHSB. The new system should be a fully integrated application that allows for future scalability to accommodate changes in laws; real-time access to current, accurate, and complete information; and security features or mechanisms that meet all current industry standards. As part of that project, CHSB should ensure that the new system provides for audit trail information for the current legacy mainframe terminal users and allows for less confusing data entry.

Auditee's Response:

> *The CHSB acknowledges the Criminal Justice Information System (CJIS) is a computer system with its primary applications written in nearly thirty-year old programming language running on an outdated mainframe computer hardware and operating system. Until Fiscal Year 2009, there has been no significant funding provided to the*

CHSB to reengineer the applications and computer systems referenced in this audit report.

CHSB recently received funding from an Information Technology Bond and immediately began the process of selecting a vendor to begin replacing the computer and software infrastructure to support the modernization of the CJIS, including the reengineering and rewriting the state's criminal history system. It is anticipated the contract to replace the current CJIS will commence on or about April 15, 2009, pending successful contract negotiations with the vendor. The new system will meet SAO recommendations as well as established state and national standards and functionality. It is expected the modernization effort will be completed within 18-24 months from this date.

The CHSB is the state agency responsible for the dissemination of criminal offender record information (CORI) in the form of criminal history to the state's law enforcement and criminal justice communities as well as non-criminal justice agencies and the general public; however the generation and maintenance of the CORI record is the responsibility of the Massachusetts court system.

The criminal history record known as the Board of Probation (BOP) file is a product made available to Massachusetts criminal justice and law enforcement user community via the CJIS application using legacy mainframe computer terminals and the more recent CJIS Web application interface. The genesis of the BOP file is the nightly electronic feed from the Massachusetts Administrative Office of Trial Court (AOTC). The CHSB has no technical ability to review this file for accuracy, nor does the agency have a statutory mandate to confirm accuracy.

Understanding that the accuracy of the criminal history record is paramount to the efficient operation of the criminal justice information system, the CHSB does maintain an official process to assist in the correction of the criminal history record if it is determined there are errors within the record, although it is the responsibility of the AOTC and Office of Commissioner of Probation (OCP) to update and /or correct the record. The CHSB has record correction guidelines posted to its public Mass.gov web site for individuals who seek to correct their criminal history record.

The CHSB has also established an Identity Theft Index for citizens who believe their identities have been used by others and a criminal record is now wrongly associated to them. Citizens may contact the CHSB to register for this service. If it is determined through investigation that a criminal history record is incorrectly associated with the individual, the CHSB will work to remedy the inaccuracies. This program is administered by the CHSB Office of Legal Counsel.

Auditor's Reply:

We are pleased management has resolved the delay in funding and has secured the necessary resources to develop and implement a new system. Since the resources necessary to proceed have been made available to replace CJIS, continued due diligence will need to be exercised over the system development and implementation process. The application of system development life cycle methodology, or good

project management techniques, will help ensure that that the right set of features and appropriate controls are built in, the system functions as intended, training and documentation are addressed, and development and implementation costs are minimized. We urge CHSB and the courts to engage in a collaborative effort to ensure that the CJIS application contains relevant and reliable information regarding criminal history records.

Although the final point of accountability for data reliability for the CARI system rests with the courts, CHSB is well positioned to monitor and seek remedies regarding data integrity since it is the state agency responsible for the dissemination of criminal history records to the state's law enforcement and criminal justice communities as well as non-criminal justice agencies and the general public. Consequently, we believe that CHSB and the courts have a shared responsibility to ensure adequate controls are in place regarding the reliability of criminal history records.

2. Access Controls over the CJIS Application Data Files

Our audit indicated that access controls over CHSB's CJIS application data files needed to be strengthened to ensure that proper authentication and active monitoring of specific users are in place to ensure only authorized and required queries of criminal history records are being performed. Our audit revealed that the current CJIS application does not provide adequate system access security for users accessing the system from dedicated terminals at remote locations. Although our audit indicated that CHSB administrative and technical personnel, remote mobile law enforcement, and Virtual Private Network (VPN) laptop users were subject to appropriate authorization, activation, and authentication controls, access through the dedicated terminals did not require users to be uniquely identified, since access was permitted on an authorized terminal basis rather than authenticating the individual users. The system's inability to authenticate individual users or sufficiently log event history information for access through dedicated terminals inhibits CHSB from administering and evaluating access and related activities on an individual basis. Moreover, CHSB did not sufficiently monitor and evaluate the nature and type of inquiries of CJIS data files and associated information to ensure that inquiries are for "legally authorized" purposes and that other types of inquiries are "strictly prohibited." Consequently, potentially unethical activities outside of authorized usage through repeated searches and queries for unlawful activity were made on celebrities and high-profile citizens through the CJIS application without any apparent work-related justification.

CHSB is responsible for maintaining the integrity of CJIS operations and for safeguarding the personally identifiable information, or PII, as it is known, for each criminal history system record. According to

CHSB management, there were over 25,000 approved users with active CJIS accounts who have access to approximately 3.4 million criminal history files for three million individuals. We determined that CHSB has policies and controls regarding criminal history records and that employees and users are trained on the restrictions for use of the system. For example, each time an employee logs onto CJIS, he or she acknowledges that the access and dissemination of records are protected by Massachusetts General Law (MGL) Chapter 6 Sections 168-172 and Code of Federal Regulations (28 CFR 20.2). These laws and regulations require that "Only authorized persons in the performance of their official duties may access, use or disseminate this information for official and lawful criminal justice purposes." Also, the Information Technology Division's Enterprise Cybercrime & Security Incident Response Policy and Procedures defines an incident as "internally or externally initiated events, intentional or accidental, that threaten or exploit an unauthorized and/or illegal use of Commonwealth electronic information systems and/or services. Such events include, but are not limited to, a criminal use of Commonwealth systems and/or services (e.g., cyber-stalking, identity theft, child pornography, etc.) as well as disclosure, destruction, and/or alteration of state managed systems or data." Unauthorized access to the Federal Bureau of Investigation (FBI) CJIS records may also constitute a violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) that prohibits unauthorized and fraudulent access to information. The Computer Fraud and Abuse Act (18 U.S.C. § 1030) states that fraud and abuse occur when a user "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any department or agency of the United States." In addition, unauthorized access may require security breach notification under MGL 93H. According to MGL Chapter 93H, "security breach" is defined as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth."

Users access these critical data files through CJIS by initiating a search that is referred to by CHSB as an event. Each event or search can be comprised of multiple queries. Each query is assigned a specific set of criteria that is relayed to the user in an electronic report. The queries include personal information, such as the offender's name, gender, and Social Security Number. CJIS offers these authorized users the ability to query the Interstate Identification Index (III) which is a national index of criminal histories in the United States that is maintained by the FBI. Included in this index are individuals who have been arrested or indicted for a serious criminal offense anywhere in the country. Search results from the III give a list of states that have criminal history on a given person.

Users also have access to the federal central database for tracking crime-related information known as the National Crime Information Center (NCIC). The NCIC is maintained by the FBI's Criminal Justice Information Services (CJIS) Division and is interlinked with similar systems that each state maintains. By using the FBI's NCIC, Massachusetts vehicle registrations and driving histories, and other databases, CJIS can tell users whether someone is wanted on an arrest warrant, is a sex offender, was reported missing, or is deemed dangerous. Authorized users can also find out where someone lives as well as confidential information, such as whether the person has a concealed weapon permit or has a sealed juvenile record on file.

Our audit determined that CHSB did not have control procedures in place for the authentication of CJIS user groups who have access to the legacy CJIS mainframe application through designated terminals. Authentication is a process to identify users and access rights to a system. Most systems require user identification codes and passwords for authentication. However, users of the legacy CJIS application through designated terminals, such as criminal justice personnel, are not required to use authentication methods. For example, when an event is instituted the standard query a law enforcement officer makes when looking for warrant information is called a Q2 query.

The Q2 query, which does not go through an authentication process, accesses several databases through CJIS, including the Board of Probation's Central File (PCF) and the Registry of Motor Vehicles' (RMV) database. The FBI's NCIC is also searched through a Q2 query. NCIC contains nationwide information on wanted and missing persons, Secret Service alerts, and threats to national security. CHSB management attributed its inability to develop security controls and to assess the system's vulnerability to an end-of-life legacy system as well as a shortage of resources.

Allowing users access to CJIS without proper authentication or adequate monitoring regarding the validity of queries increases the risk of improper use of CJIS data that can lead toward data security breaches of criminal history record files. In fact, our preliminary audit tests of one local celebrity's record revealed 128 events, by dozens of CJIS users, comprised of 968 queries against this individual's personal information. For this individual, queries included multiple FBI III and NCIC record searches. In addition, users accessed data files to determine whether the individual had a Massachusetts Board of Probation (BOP) Criminal Case Record, an outstanding warrant, or had purchased any firearms. Users also accessed the individual's RMV picture image and license number inquiry that included the current home address.

We note that CHSB did not bring to our attention whether any confidential data was disseminated outside the agency. However, CHSB could not provide any explanation or purpose to justify the checking of this

celebrity's name through CJIS or for authorizing those searches. Authorized CJIS users sign an "Agreement of Non-Disclosure" stating "data found within, or made available through the criminal justice information system (CJIS) is provided to criminal justice agents and agencies for the performance of their legally authorized, required functions. Inquiries and other types of transactions, which are not done pursuant to a criminal justice purpose, are strictly prohibited." Disciplinary action, up to and including dismissal and/or criminal prosecution may result in misuse of the state and FBI CJIS data files.

Initially we had believed that group users, that could not be identified as specific individuals, who had accessed legacy CJIS data files through the dedicated terminals accounted for the majority of inappropriate or unethical activities that were outside of authorized usage. However, subsequent testing revealed that users were accessing unauthorized data files from all entry points into the system through the CJIS web, including non-CHSB administrative and technical personnel, remote mobile law enforcement, and Virtual Private Network (VPN) laptop users. Our subsequent tests determined that there were dozens of events that included hundreds of queries or "hits" made on the names of selected famous Massachusetts people accessed through the CJIS web. Between January 1, 2008 and December 15, 2008, our audit determined that individuals authorized to use CJIS accessed computer files on local celebrities and high-profile citizens, apparently without work-related justification.

Personal information available through CHSB's computer system goes far beyond background information normally associated with an individual's criminal record. Law enforcement personnel can access government agency files on individuals' driving records, birth dates, ownership of vehicles, physical descriptions, Social Security Numbers, restraining orders and, in some cases, threatened or attempted suicides while in police custody. According to CHSB management, the extended age of the CJIS application has made it difficult to implement any important program changes including enhancing security controls for the CJIS WAN. A new system with a single architecture that does not have multiple access and event data logs should make it easier for CHSB to identify unusual or highly sensitive queries. We understand that additional revenues are needed to institute an appropriate level of monitoring and evaluation of CJIS web data requiring increased staffing in that functional area. However, a more comprehensive process for the monitoring and evaluating of user access needs and associated queries needs to be implemented.

Although CHSB indicated that it was not aware of the extent of the problems regarding unauthorized access to data files, it is our understanding that CHSB has begun investigations of possible security breaches regarding the disputed queries that were uncovered by the audit team. MGL Chapter 93H identifies personal information as "a resident's first name and last name or first initial and last name in

combination with any 1 or more of the following data elements that relate to such resident: (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account."

Recommendation:

We recommend that CHSB strengthen access controls over CHSB's CJIS application data files to help ensure that unauthorized dissemination of personally identifiable information does not occur. We also recommend that CHSB implement breach notification policies, procedures, or other criteria for reporting incidents of unauthorized access of criminal history records when they are detected. This should include guidance on the various steps to be followed and decisions to be made in response to a potential incident of unauthorized access to criminal history records and offender personally identifiable information, and an agency-wide PII breach response policy.

CHSB should institute monitoring and evaluating procedures to ensure that only required and justifiable queries are being performed and that unusual activity is identified regarding access to CHSB information for high-profile individuals. We also recommend that CHSB conduct the necessary vulnerability and risk assessments of all systems that are accessed through CJIS given the weaknesses and data vulnerabilities identified in this review of CJIS. Accordingly, we further recommend that CHSB should make resources available to conduct the assessments as soon as possible.

Concurrently, we recommend that if CHSB finds that CJIS data were improperly disseminated or accessed, that the Board follow the requirements for security breach notifications under MGL Chapter 93H, which include:

- A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information,
- The number of Massachusetts residents affected as of the time of notification,
- The steps already taken relative to the incident,
- Any steps intended to be taken relative to the incident subsequent to notification,
- Information regarding whether law enforcement is engaged investigating the incident, and
- A determination of whether the incident must be reported to other state and/or legal authorities.

Auditee's Response:

> *CHSB acknowledges the SAO report findings of questionable inquiries into the CJIS and has taken steps to begin to notify the CJIS user agency heads of these concerns*

and will request that an internal inquiry be initiated to determine whether these queries are for official criminal justice purposes.

Access to the CJIS is restricted to authorized criminal justice and law enforcement personnel for official criminal justice purposes only. While the CHSB maintains authority and responsibility for maintaining the CJIS, and oversees policy compliance on behalf of the FBI for national criminal history, the CJIS operates under a shared management concept. The CHSB delegates authority to the CJIS User Agency Head through a shared management concept. In summary, CJIS user agencies such as police departments enter into a User Agreement with the CHSB in which the policies, procedures and responsibilities are articulated and accepted.

The respective agency head is responsible for local management for access to and use of the CJIS including maintaining a local CJIS user policy that addresses access, security, dissemination, training and reporting of security violations to the CHSB. Under CHSB policy all CJIS users are required to be trained, tested and certified in the use of these systems at least every two years. This process is managed by the local department.

The CHSB and FBI traditionally conduct triennial on-site audits and mail audits of all CJIS user agencies to ensure policy compliance. A proactive audit program is in effect as well, in which CJIS operations staff randomly contacts a CJIS user agency to confirm the identity of the CJIS user who made a query and to document the purpose of the CJIS query. CHSB also provides policy compliance training to agencies at biannual regional CJIS user meetings.

Access to the criminal history file known as the BOP is password-protected on both legacy and newer CJIS web applications. An audit log is maintained on all transactions conducted within the CJIS. The SAO correctly points out that certain queries within the legacy mainframe such as the Q2 function which is an integrated query that checks local and national missing and wanted persons files, driver license information and criminal history summary information is not password protected; however, the audit log captures the exact date, time, station number the query originated from and the location of the CJIS terminal the query originated from. Policies and procedures are in place at the CJIS user agency that would assist the CHSB to determine the user of the legacy system at a particular date and time.

The SAO report expresses concern that sensitive data can be viewed, destroyed or altered accidentally or deliberately. In this regard, there are policies and procedures in place that address these issues if they occur. There is no ability for the CJIS user to alter the criminal history record, as this is a view only file generated by the AOTC/OCP. There are several files that CJIS users can enter data into such as warrants, stolen vehicles or missing persons. Each of these record entry processes require a second party check in which another agency employee is required to check for accuracy and completeness. It should be noted that in the seven years I [Curtis Wood, Executive Director] have been with the CHSB there has never been an instance or report of data being altered or destroyed.

Concerning viewing sensitive data, only authorized users are allowed access to the systems under controlled environments. Legacy CJIS terminals as well as CJIS Web access points are located within secure law enforcement or criminal justice locations. All CJIS user agencies are required to follow CJIS/NCIC security policies.

Access to the CJIS is for official criminal justice purposes only. CJIS users are provided training in this policy requirement and there is an expectation of adherence to the CJIS policy. Under the shared management concept, the CJIS user agency head is responsible for the local management control of the systems. In the event the CHSB is notified or learns that a violation of the CJIS policy occurs, the CHSB will initiate an investigation into the circumstances and request the CJIS user agency head to conduct an internal inquiry to determine the circumstances of the alleged violation and report the findings to the Office of Legal Counsel and the CJIS Systems Officer. There are sanctions in place for violations of the CJIS/NCIC policy and CORI statute.

Auditor's Reply:

We acknowledge that CHSB management recognizes the need to enhance the current security and access controls for the CJIS system. Monitoring the access of dissemination of sensitive and confidential information must be on a continuous basis. System security should include strong authentication controls and detailed audit trails to log all access events and related actions, such as the access to or modification of sensitive and confidential information. The set of security controls should be sufficiently comprehensive to detect unusual activity and clearly identify users who query information from CJIS. In the design of the new system, CHSB management should ensure that appropriate administrative and technical controls are designed to provide a higher level of assurance that security and confidentiality objectives are addressed.

Although CJIS management has delegated authority to CJIS user agency heads for monitoring CJIS use, CHSB, because of its assigned primary functions, must retain responsibility for monitoring compliance with established policies and procedures regarding access to and data integrity for the CJIS application. CHSB's response indicates that "the audit log captures the exact date, time, station number the query originated from and the location of the CJIS terminal the query originated from." As such, monitoring functions and detection controls should be routinely performed to ensure that queries of the CJIS application are for justifiable and legal purposes.

3. Program Change Controls

Our audit determined that CHSB had not developed a comprehensive change process for the CJIS application. As a result, CHSB could not ensure that changes to CJIS program files and database software were authorized, received, approved, and properly tested. Not following formal change control

procedures increases the risk of unauthorized changes to production data, inadequate monitoring of production data, and inadequate documentation to support system maintenance and future system enhancements.

Program change control procedures are meant to ensure changes are made in a controlled environment to protect system software integrity. System software modifications should be authorized and properly tested for required system parameters to prevent unauthorized changes to applications or data and to prevent malfunctions during processing runs. Further, documentation of system changes is important to help ensure that personnel making future changes will understand all aspects of previous changes. According to the Commonwealth's Information Technology Division, agencies should have a standard procedure for identifying, selecting, installing, and modifying system software to meet operational needs. Additionally, a written standard should exist for testing new versions, products, and changes to system software before implementation.

CHSB has no formal application, approval process, or database that is maintained for program changes or modifications. Our audit determined that the current informal process requires that the CIO and CJIS Operations Manager be notified if a program change is needed. The CIO and CJIS Operations Manager communicate via email with the proper CHSB division assigned to the project (normally the Programming Division) and meet to discuss what needs to be done. Once the modifications are available on a test system, the CIO and CJIS Operations Manager either conduct the testing of the program change or assign it to specific CHSB personnel. If assigned out, the CIO and CJIS Operations Manager receive written correspondence via email as to whether the program change may be implemented into production. Once the changes are moved to production, the CJIS Operations Division provides another round of testing. The CIO and CJIS Operations Manager then schedule the rollout of the program change in accordance with CHSB's CJIS Scheduled Maintenance policy.

Although we determined that there is no formal application or database maintained, there was a history of the stated changes or modifications within an email trail. This method is useful for change notification, but makes it very difficult for a user to find the answer to a specific question about using the system. Also, the email method makes training new staff particularly difficult because notices are not compiled into a single reference or training manual. CHSB indicates that it has recognized its inadequacies of not maintaining a central repository of program changes and is currently working on a procedural statement as well as creating a central repository to maintain this information. We found that CHSB, during the audit, began making improvements to the organizational policies and procedures related to the change control process. For example, online requesting and tracking of changes was being instituted, which will

be a great improvement over the manual process. In addition, the new online system will provide more documentation of management approvals than the previous system did.

Recommendation:

To ensure adequate management of the maintenance and updating of CJIS, CHSB should:

- Develop written change control policies.
- Develop a policy requiring the system supervisor to approve in writing incorporation of software changes into the production software. This is necessary to reduce the risk of a programmer inserting untested or poorly tested modifications into the production software. Also, this approval process would give CHSB a change control log that would document each change instituted in the production software.
- In the case of significant changes, require, when appropriate, that formal user acceptance tests be performed before the final changes are allowed to be incorporated into the production software.
- Require staff to update user operation manuals when changes are made to the software impacting the operation of the system.

Auditee's Response:

> *Regarding the SAO findings and recommendations concerning program change control procedures, CHSB agrees with the findings and recommendations. The agency has begun addressing these issues and will introduce and maintain a new system of change control by the end of the fiscal year 2009.*

Auditor's Reply:

We commend CHSB's efforts to ensure that any future program change controls will be properly tested for adequate system parameters to help prevent unauthorized changes to the application system. To the extent feasible, documentation of previous program changes should be enhanced to provide a detailed explanation of system modifications.

4. Off-Site Storage of Backup Media

CHSB did not maintain backup copies in a secure off-site storage location of any electronic files or documents, including its critical CJIS files. At the time of our audit, CHSB stored its backup tapes in its computer room. CHSB senior management decided not to store a copy of the CJIS database off site because of the "inability to replicate the hardware/operating system platform due to the unavailability of manufacturer's equipment due to age of system." Although the Administrative Office of the Trial Court (AOTC) maintains the Criminal Activity Record Information (CARI) database that serves as the

origination of the CJIS database, CHSB stated that the "ability to disseminate the information as prescribed by statute and our mission would be compromised." During the audit, CHSB performed the migration of the CJIS database into an Oracle database environment to meet operational needs and was working to locate a copy of the CJIS database off site at a State Police facility.

Backup tapes should be stored in an off-site storage area in order to minimize reliance solely on a single set of backup media and to help ensure recoverability of IT systems should the on-site backup copies become damaged or unreadable. In addition, CHSB had not tested backup systems or data to ensure that automated systems and data files could be properly restored in the event of a disaster. As a result, critical data may not be recoverable in the event of system failures. Backup and recovery procedures are a critical component of the information services function and help ensure continued operations. Generally accepted backup and recovery practices state that backup and off-site storage plans should:

- Document backup procedures for software and data files.
- Document procedures for off-site storage and the availability of all material that would be required to restore and recover critical business functions within their identified maximum outage time periods.
- Ensure that appropriate retention cycles have been established for critical off-site storage documentation based on the business needs and risks.
- Require periodic testing of off-site backup files to ensure the material required to resume/recover critical business processes is available.
- Ensure that information technology staff and division managers have approved backup and off-site storage procedures.
- Document procedures for restoring systems from backup copies of software and data files.

Disaster recovery and business continuity planning are necessary to ensure that services will be received and provided in the event of a disruption. Disaster recovery and business continuity plans should include procedures to generate backup copies of information system programs and data on a scheduled basis and a copy on-site and an additional copy stored in a secure off-site location to ensure redundancy. Without adequate disaster recovery and contingency planning, CHSB would not be able restore critical information systems that provide vital business functions in a timely manner.

Recommendation:

We recommend that CHSB management store backup copies of software and data files in a secure and easily accessible off-site location, and establish procedures that any authorized staff can store and retrieve backup media. We also recommend that CHSB develop and document backup, recovery, and off-site

storage procedures for critical data files, applications, media, documentation, and other information technology resources to support the recovery and resumption of business processes and system operations. The procedures should require that backup copies are tested for the recovery of applications and data on-site and off-site, backup copies are subject to appropriate librarian controls, and there is adequate segregation of duties for personnel responsible for generating and storing backup copies of electronic files, including its critical CJIS.

Auditee's Response:

> *Regarding the off-site storage of data and systems CHSB agrees with the SAO findings and recommendations. The agency is developing a new protocol in this regard. For the interim, the CHSB will store its back up data at the Massachusetts State Police General Headquarters (GHQ) in a secure area. For the long term, the CHSB will operate a back up system at the proposed second data center in Springfield, MA.*

Auditor's Reply:

We are pleased that CHSB is taking action to implement storage of backup copies at a secured off-site location. We believe that this will address a serious deficiency in disaster recovery and business continuity planning. We agree that in the long term, CHSB should use the proposed second data center in Springfield as a secure off-site storage location.

5. Inventory Controls over Computer Equipment

Our audit disclosed that inventory controls over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in CHSB's inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. We found that controls needed to be strengthened to update the inventory record when equipment is relocated, disposed of, or lost or stolen. We also found that inventory records were not being adequately reviewed for accuracy and completeness, and that an appropriate level of reconciliation had not been performed for the past six years. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders CHSB from properly accounting for IT resources, evaluating the allocation of equipment, identifying missing equipment, and supporting IT configuration management.

Although we determined that CHSB had documented internal controls regarding the purchasing and receiving of IT resources, we found that documented policies and procedures needed to be enhanced

regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. For example, although documented procedures were in place requiring an annual inventory to be conducted at the end of each fiscal year, CHSB could not provide documentation to demonstrate that an annual physical inventory had been taken. Furthermore, although CHSB had adequate policies and procedures for the disposal of surplus property and Chapter 647 requirements, they were not being followed as evidenced by the failure to submit reports to the Operational Services Division's State Surplus Property Officer and the Office of the State Auditor, respectively.

Our analysis of CHSB's inventory system of record for computer equipment indicated that most of the appropriate data fields, including description, identification tag, user name, serial number, and location, were present. However, there was no data field for historical cost, as is required by Commonwealth of Massachusetts regulation for all departments to provide a comprehensive, auditable inventory record of fixed assets. By failing to record the historical cost of purchased computer hardware items and their purchase dates on CHSB's inventory system of record, CHSB was not in compliance with the Office of the State Comptroller's (OSC) 2005 fiscal year fixed-asset requirements and OSC Memorandum No. 313A.

With respect to the recording of IT-related assets, we found that CHSB lacked appropriate and adequate management oversight to prevent and detect errors in the recording of identifying data for received computer equipment into CHSB's inventory system of record for IT equipment. Our tests indicated a significant error rate and inconsistencies in identifying data recorded on CHSB's computer hardware inventory listing. Specifically, our audit tests were performed on 27 computer hardware purchases consisting of 101 purchased computer equipment valued at $257,899 selected from fiscal year 2007 and 2008 invoices. Our audit test revealed that 58 of the 101 items, representing an error rate of 57%, were not included in CHSB's system of record. Our audit tests of CHSB's system of record for IT-related equipment indicated weaknesses in the accounting of computer equipment. CHSB provided an inventory system of record that listed 1,225 IT-related assets as of May 8, 2008. Based on a randomly selected sample of 71 items of computer equipment selected from the inventory record, we attempted to verify by inspection the existence and the recorded location of the computer equipment. We found that 50 pieces of computer equipment were not at the locations indicated on the inventory record and could not be found by CHSB. Of the 21 items that were located, all were properly tagged, and the inventory system of record correctly listed tag and serial numbers and location.

To verify the integrity and completeness of the inventory system for computer equipment, we randomly selected 46 additional items of computer equipment from actual floor locations and determined whether

all items were listed on CHSB's system of record. We found that of the 46 items selected, 24 (52%) of the selected items were not recorded on the inventory record. With respect to these items, there was no documentation available to support whether the equipment was properly disposed of in accordance with the Operational Service Division's (OSD) Surplus Property policies and procedures. In addition, our audit test of all notebook computers indicated that of the 66 notebook computers tested, a total of 31 notebook computers (47%) purchased by CHSB between 1996 and 2001 could not be found. However, we were able to determine that six of the sample items drawn from the system of record had been designated by CHSB as surplus. The lack of a complete inventory of computer equipment hinders CHSB's ability to properly account for available hardware systems and undermines its ability to detect missing or stolen equipment.

Because of the rate of data input errors, failure to record asset costs and acquisition dates, and inadequate management of the system of record, an acceptable level of data integrity did not exist for CHSB's inventory system of record for IT equipment at the time of our audit. CHSB needs to ensure that appropriate controls are in place and in effect for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory database. Without formal, documented, and tested procedures for performing an annual physical inventory count and reconciliation of the inventory record to purchase or lease documentation and surplus equipment records, CHSB management cannot be adequately assured that its computer equipment is properly accounted for and that the inventory record is comprehensive, timely, and accurate. In addition, a periodic comparison of the computer equipment and the recorded accountability of the computer equipment will reduce the risk of unauthorized use, loss, or theft of computer equipment. We believe that the weaknesses in inventory control were the result of lack of adequate monitoring, management oversight, and proper assignment of inventory control responsibilities.

Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989 states, in part, that "the agency shall be responsible for maintaining accountability for the custody and use of resources and assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

Recommendation:

To ensure that the inventory of computer equipment is adequately maintained, we recommend that CHSB strengthen its current practices to ensure compliance with policies and procedures documented in the OSC's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," its associated internal control documentation, and OSD's guidelines regarding the accounting for and disposal of property and equipment. CHSB should also implement these control procedures to help ensure that all IT-related equipment is recorded on the inventory record in a complete, timely, and accurate manner so that CHSB can maintain a comprehensive record of all IT-related equipment on a perpetual basis. In addition, CHSB should comply with Chapter 647 of the Acts of 1989 and immediately report all instances of unaccounted-for variances, losses, and thefts of funds or property to the Office of the State Auditor. CHSB's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

CHSB should document a formal process for the assignment and return of notebook computers. Users should be required to formally sign-out and sign-in each notebook computer and record the actual date of transfer of responsibility. CHSB's designated fixed-asset manager for IT resources should periodically review the status of notebook computers, especially those that have been signed out. We recommend that CHSB perform an annual physical inventory and reconciliation of its IT resources to ensure that a relevant and reliable inventory record of IT resources is in place. We recommend that the inventory system of record be periodically verified through reconciliation to physical hardware, acquisition, and disposal records. The reconciliation and improved documentation will help ensure the integrity of CHSB's perpetual inventory system of record for IT-related assets, provide reasonable assurance that the inventory records can be used to support IT configuration management, and help safeguard computer equipment. We further recommend that CHSB's system of record for IT inventory be expanded to include data fields containing information relative to cost, condition, acquisition and installation dates, and status of the IT resource.

Auditee's Response:

> *Regarding the findings and recommendations concerning the agency's inventory control system, CHSB is taking immediate action to address these areas and will be in compliance with all Commonwealth regulations, procedures, protocols and best practices by the end of this fiscal year. Over the last several years CHSB determined much of its desktop and laptop computer equipment procured during the 1996-2001 time period was of no value and disposed of these systems under established Commonwealth guidelines through a state contractor. Prior to disposal of any CHSB computer equipment the devices are sanitized of all data, or the hard drives are destroyed under supervision.*

The SAO report finds that certain equipment procured during this same 1996-2001 time period could not be located and no paperwork was found to substantiate that proper disposal procedures were followed. The CHSB acknowledges this finding, but also offers there is currently no associated value to these systems due the age (8-13 years old). CHSB recognizes its inadequate record keeping in this instance and has begun a complete review of its internal control policy and inventory management process to immediately strengthen its process.

In closing, CHSB accepts the formal report provided by the SAO and will commit the resources to address all of the findings.

Auditor's Reply:

We commend the actions initiated by CHSB to improve its fixed-asset inventory controls. We believe that a single comprehensive inventory control system for all CHSB fixed assets is an important ingredient for CHSB's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding fixed assets and assist CHSB in making IT infrastructure and configuration management decisions.

We believe that controls to ensure adequate accounting of fixed assets will be strengthened by updating the inventory record when changes in status or location occur and reconciling the physical inventory to the system of record on a routine or cyclical basis. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection of lost or stolen equipment and the subsequent accounting for surplused equipment. In addition, these efforts should help improve the current status of equipment for configuration management purposes.

CHSB needs to ensure that proper documentation is in place regarding the proper sanitation of surplused equipment. Since it is unlikely that the data contained in laptops that are misplaced or stolen would have been sanitized, we recommend that CHSB exercise appropriate encryption techniques for any data contained in laptop computers.