The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2008-0026-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE BUREAU OF STATE OFFICE BUILDINGS

April 1, 2005 through February 12, 2010

OFFICIAL AUDIT REPORT

JUNE 30, 2010

TABLE OF CONTENTS

INTRODUCTION

The Bureau of State Office Buildings (BSB) was established and organized under Chapter 8, Section 1, of the Massachusetts General Laws and operates within the purview of the Executive Office for Administration and Finance under Chapter 7, Section 4G, of the General Laws. According to BSB's mission statement, its primary purpose is "to provide a safe, secure, workplace for state employees and customers" and to "efficiently maintain mechanical systems and buildings within budget, recognizing that they function as places of business, museums of art and history, and sites of public congregation."

BSB manages the Government Center complex of state office buildings located in Boston that includes the State House and the John W. McCormack, Charles F. Hurley, and Erich Lindemann buildings. The BSB, which has its headquarters located at the State House in Boston, also manages a building in Pittsfield and a building in Springfield. BSB received an appropriation of $14,752,903 for fiscal year 2008 and $15,349,041 for fiscal year 2009. At the beginning of our audit, BSB was staffed by a Superintendent and 42 employees, including two deputy superintendents and an IT coordinator. Subsequent to our audit, the BSB's staff had been reduced to 37 employees with the IT coordinator no longer reporting within BSB as a result of the IT consolidation efforts within the Executive Branch. The Superintendent, who is appointed by the Governor, is responsible for the administration of BSB's programs and services.

The BSB is organized into functional areas, as follows: Administration, Finance, Planning and Engineering, Security/Parking/Safety, ADA Compliance, Events Planning and the Arts Commission, and Building Operations. The BSB oversees the operations of the State House and monitors building system performance including the management of private contracts for cleaning, grounds, fire alarm system, security, and pest control. The BSB also oversees mechanical maintenance of its facilities including elevators and heating ventilation air conditioning (HVAC) systems. The BSB works closely with personnel in the legislative and executive branches. The Divisions of Planning and Engineering and Building Operations oversee mechanical maintenance of BSB's Boston facilities, including the elevators and the HVAC systems. These areas also evaluate and address building requirements, such as operating and capital expenditures, oversight of related construction projects, and management of air quality for the BSB buildings.

The goal of the Division of Security, Safety, and Parking is to ensure a safe and secure workplace for employees and state building customers by managing security contracts, training occupants on emergency evacuation procedures, and managing the photo ID access card system. The functional area is responsible for parking operations and the locks, anti-intrusion devices, and surveillance equipment. The

area is also charged with the maintenance of fire protection and safety systems for the state buildings under BSB's charge. BSB's Administration and Finance Division, in conjunction with the Executive Office for Administration and Finance, provides management oversight for the BSB's activities in terms of procurement, information technology, human resources, legal compliance, and budget control. The Events Planning and Arts Commission has curatorial responsibility for State House art and manages and schedules State House events.

Information technology resources that support the BSB's business operations are comprised of a local area network (LAN) consisting of two file servers and 46 workstations. Through BSB's connection to MAGNet, the Commonwealth of Massachusetts wide area network (WAN), the BSB's staff can access the Commonwealth's Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

BSB uses two commercial systems, FAMIS and Metasys. FAMIS, which is maintained by Division of Capital Asset Management, is an application system that primarily consists of work order records. The Metasys system uses the state's WAN to supervise and manage the building systems in Boston, including HVAC, fire detection and alarms, elevators, environmental monitoring, preventative maintenance, and work orders. BSB's Security/Parking/Safety functional area uses the physical access card system to help manage the process of distributing physical access cards for entry to certain state buildings. At the time of our audit, one BSB employee was responsible for general IT systems and another employee was responsible for security systems.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Bureau of State Office Buildings (BSB). The audit, which was conducted from June 2, 2008 to November 26, 2008, and from November 16, 2009 through February 12, 2010, covered the period of April 1, 2005 through February 12**,** 2010. Our audit scope included an examination of IT-related general controls pertaining to IT policies and procedures, physical security, environmental protection, inventory control of computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media.

Audit Objectives

Our primary objective was to determine whether IT-related controls were in place and in effect to support BSB's IT processing environment. In this regard, we sought to determine whether BSB's IT-related internal control environment, including policies, procedures, and practices, provided reasonable assurance that control objectives would be achieved to support business functions.

Our audit objective regarding IT policies and procedures was to determine whether the policies and procedures addressed under our review were sufficiently documented and in place. We determined whether adequate physical security controls were in place and in effect to provide reasonable assurance that only authorized personnel had physical access to IT resources to prevent unauthorized use, damage, or loss.

We evaluated whether appropriate environmental protection controls were in place to provide a controlled operating environment to prevent and detect damage to IT resources. Our objective regarding inventory control was to determine whether computer equipment under BSB's charge was properly accounted for in an inventory system of record. Our objective regarding system access security was to determine whether adequate controls were in place to provide reasonable assurance that only authorized users were granted access to BSB's access card system.

With respect to the availability of automated processing capabilities and on-going access to IT resources and data, we determined whether business continuity controls would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In conjunction with reviewing business

continuity planning, we determined whether proper backup procedures were being performed and whether backup copies of magnetic media were stored in secure on-site and off-site locations.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of the mission and business objectives of the Bureau of State Office Buildings. To gain an understanding of the primary business functions that were supported by the automated systems, we conducted pre-audit interviews with managers and staff and reviewed BSB's enabling legislation, website, and selected documentation provided by the BSB. We gained through interviews a high-level understanding of the information technology used to support BSB's business operations. We documented the significant functions and activities supported by the automated systems and reviewed automated functions that were related to mission-critical or essential operations.

We interviewed BSB's management regarding internal controls for physical security and environmental protection over and within the operations and engineering offices, the file server room that housed computer equipment in Boston, and the on-site and off-site storage areas for backup copies of magnetic media. We inspected the operations and engineering offices and the file server room, reviewed relevant documents, and performed selected preliminary audit tests. In conjunction with our review of internal controls, we performed a high-level analysis of risks and threats to selected components of the IT environment. We developed our audit scope and objectives based on our pre-audit work.

Regarding our review of IT policies and procedures, we interviewed senior management and staff, completed questionnaires, and reviewed and analyzed existing IT-related policies and procedures. We determined whether an up-to-date internal control plan was in place and included or made reference to IT control policies and whether IT internal controls were adequately documented. We assessed the extent to which existing documented policies and procedures addressed selected IT functions.

We determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining physical access to the operations and engineering offices and the file server room. We reviewed control procedures for physical access, such as the authorization of staff to access the file server room, and key management regarding door locks for the file server room and other areas housing IT equipment. We conducted walk-throughs, observed and identified security devices, and reviewed procedures to document and address security violations and/or incidents. To determine whether computer equipment and backup copies of magnetic media stored on-site and off-site were adequately safeguarded from damage or loss, we reviewed physical security over the IT resources through observation and interviews with senior management.

With respect to environmental protection, our objective was to determine whether adequate controls were in place to prevent and detect damage to, or loss of, computer equipment and media. To determine the adequacy of environmental controls, we conducted walkthroughs of the file server room and office areas housing IT equipment at BSB's main office. Our examination included a review of general housekeeping; fire prevention, detection and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of pertinent documentation.

To assess the adequacy of disaster recovery and business continuity planning, we evaluated the extent to which BSB had recovery plans to resume IT operations should the network and servers be rendered inoperable or inaccessible. We interviewed senior management to determine whether BSB had formally documented procedures for the development and maintenance of appropriate disaster recovery and business continuity plans. We determined the extent to which BSB had performed a risk analysis and assessment of business impact with regard to the loss of IT-enabled business operations under different disaster scenarios. As part of our examination of business continuity planning, we assessed the adequacy of the generation and storage of backup copies of magnetic media, and evaluated physical security and environmental protection controls for on-site and off-site storage. In that regard, we interviewed IT staff responsible for generating and storing the backup copies. We further sought to determine whether BSB's IT staff were aware of, and trained in, all procedures for restoring systems including the use of backup copies of software and data files that would be required under disaster or emergency circumstances.

With regard to inventory control over computer equipment, we evaluated whether an annual physical inventory was conducted, whether computer equipment was accurately recorded and reconciled, and whether the inventory system of record was properly maintained for computer equipment. To evaluate whether adequate controls were in place and in effect to properly account for BSB's computer equipment, we determined whether sufficiently detailed inventory control policies and procedures were in place and reviewed BSB's inventory listing of computer equipment.

We performed data analysis on the inventory system to identify any duplicate records, unusual data elements, or missing values or data. To determine whether BSB's computer equipment was properly recorded on the inventory listing, we selected 38 items (40%) of the total population of 96 recorded items from the IT inventory listing as of June 30, 2008 and confirmed their location and verified the descriptive data for each item. To further evaluate the accuracy and completeness of BSB's inventory listing, we selected an additional eight IT-related items in adjacent locations to the 38 items of computer equipment and determined whether they had been properly assigned asset numbers, and were tagged and recorded on the inventory system of record. In addition, we reviewed the inventory listing to determine whether it

contained appropriate data fields to identify, describe, and indicate the value, location, date of purchase, date of installation, assigned users, serial numbers, equipment condition, and other related information for the computer equipment.

To assess BSB's compliance with the Commonwealth of Massachusetts regulations for accounting of assets, we determined whether there was supporting evidence of BSB's performance of an annual physical inventory of IT resources. Furthermore, to determine whether BSB had complied with 802 Code of Massachusetts Regulations (CMR) 3.00 for the Disposition of Surplus State Property, we reviewed records and supporting documentation for computer equipment disposed of during the audit period. Finally, to determine whether BSB's staff were aware of and in compliance with the requirements of Chapter 647 of the Acts of 1989 for reporting missing or stolen assets, we reviewed documented inventory control policies and procedures and interviewed senior management to determine whether BSB had had any incidences of missing or stolen IT-related equipment during the audit period, and verified whether any incidents were properly reported to the Office of the State Auditor in a timely manner.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included Office of the State Comptroller's Fixed Asset Guidelines and the Information Systems Audit and Control Association's management policies and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued in July 2007.

In accordance with generally accepted government auditing standards and applicable state law, certain information gathered during this audit has been prohibited from general disclosure for security reasons. Such sensitive information is being provided in a separate audit report (No. 2008-0026-4T1) only to cognizant officials for their consideration and action.

AUDIT CONCLUSION

Based on our audit of the Bureau of State Office Buildings (BSB), we found that internal controls were in place to provide reasonable assurance that IT-related control objectives would be met regarding logical access security to IT systems, physical security and environmental protection for BSB's file server room, and on-site and off-site storage of backup copies of magnetic media. However, we found that controls for disaster recovery and business continuity planning needed to be strengthened to provide reasonable assurance that IT systems operated by BSB could be restored and business operations regained within an acceptable period of time. We also found that controls needed to be implemented to ensure that computer equipment would be properly accounted for and that the inventory system of record would be maintained.

Although certain controls were in place, the level of formal documentation of IT policies and procedures at the beginning of our audit needed to be enhanced for physical security, environmental protection, systems access security, inventory control of computer equipment, and disaster recovery and business continuity planning. Subsequent to our initial audit work, the BSB developed operational policies, including some that were specific to IT activities. Although the policies, dated January 2009, included IT-related policies, we noted that they needed further enhancement. The absence of sufficiently documented policies and procedures increases the risk that desired control practices would not be adequately communicated, administered, enforced, or evaluated.

We found that physical security controls were in place to safeguard the BSB's IT resources from unauthorized access. In addition, adequate environmental protection, such as fire detection and suppression controls and a dedicated air conditioner, were in place in BSB's file server room to support a proper operating environment and help prevent damage to, or loss of, IT resources. All the servers hosting the databases used by BSB have been provided with an uninterrupted power supply and dedicated cooling systems. We also observed that the BSB's file server room was neat and clean, temperature and humidity levels were appropriate, and that emergency shutdown procedures were available. With respect to the John W. McCormack Building, BSB had upgraded the electrical services in November 2006 to provide backup generator support for all computer rooms within the building.

Our audit disclosed that BSB did not have a formal, tested, disaster recovery plan to provide reasonable assurance that the BSB's mission-critical access card system could be recovered effectively and in a timely manner should a disaster render the computer system inoperable. At the time of our audit, BSB had an informal Continuity of Operations Plan (COOP), but had not developed a disaster recovery strategy or business continuity plan to address the loss, or prolonged delay, of mission-critical and

essential IT operations. Furthermore, a user area plan had not been developed to document the procedures to be followed by non-IT staff in the event of a loss of IT operations. Although the BSB's draft COOP identified two potential alternative processing locations, neither had been formally designated as an alternate processing site. We confirmed that backup copies of data files for the access card system had been generated and were stored at an off-site location.

With respect to inventory control of computer equipment, at the beginning of our audit we found that the BSB was not in compliance with the Office of the State Comptroller's fixed assets policies and procedures since BSB had neither maintained an inventory system of record for property and equipment nor conducted an annual physical inventory and reconciliation. However, during the course of our audit, BSB developed an inventory listing of computer equipment. Our review of the inventory listing as of June 30, 2008 disclosed that although all items selected for review were locatable, the records of individual items of computer equipment did not include tag numbers and serial numbers. An improved inventory listing, developed as of November 30, 2009, included tag numbers and serial numbers; however, information for several data fields remained incomplete. BSB personnel indicated that certain information still needed to be entered into the system of record for computer equipment.

.

AUDIT RESULTS

1. Disaster Recovery and Business Continuity Planning

Our audit revealed that although off-site storage of backup media had been implemented and the process of identifying an alternate processing site had been initiated, the Bureau of State Office Buildings (BSB) did not have a documented business continuity plan to sufficiently detail disaster recovery strategies for IT systems under its charge. We determined that further effort is needed to develop and subsequently test a detailed recovery strategy to provide reasonable assurance that mission-critical and essential business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. In addition, while it was understood that a loss of IT capabilities would adversely impact operations, the relative criticality of automated systems needed to be assessed and the extent of potential risk and exposure to business operations needed to be documented.

BSB relies on technology to administer the access card system and to manage Heating Ventilation and Air Conditioning (HVAC) for the maintenance of the six buildings that are under its charge located in Boston, Pittsfield, and Springfield. With respect to the system that manages HVAC, the IT system, which is managed by a contracted vendor, is operated from a central operations center within the John W. McCormack building. Although the IT recovery strategy would be executed by the contracted vendor, the BSB should have contingency plans in place to outline the actions that BSB staff would take should the systems supporting HVAC be rendered inoperable for an extended period. Periodic communication with the vendor is also essential to ensure that adequate disaster recovery plans are in place for this mission-critical function. According to BSB management, in the summer of 2009 the BSB initiated a planning process in collaboration with the Executive Office for Administration and Finance and the Information Technology Division with the objective of connecting vital building systems to separate and secure servers.

With respect to the access card system, which is operated and under the charge of BSB, the BSB should have documented recovery strategies and contingency plans in place to regain operation of the security system. Since the access card system is located in the State House, should its immediate location and the system be damaged, the BSB would require a backup processing site to issue cards and manage building security.

At the time of our audit, BSB's senior management had determined that the BSB would use one of its six building locations as an alternate processing site. The primary purpose of the alternate processing site would be to serve as a backup location within which IT systems could be recovered and BSB operations

could be regained. When not used as an alternate processing site, the location could be used to support off-site storage of backup media and other required resources.

The objective of business continuity planning is to help ensure the timely recovery and continuation of mission-critical and essential functions should a disaster cause significant disruption to IT and business operations. Generally accepted industry practices and standards for computer operations require that an ongoing business continuity planning process be in place that assesses the relative criticality of information systems and develops appropriate recovery and contingency plans as needed. Disaster recovery and business continuity planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality, recovery requirements, or other factors, such as risk, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

The business continuity plan should document BSB's recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. The recovery plan should contain all pertinent information, including clear delineation of key personnel and their roles and responsibilities, needed to effectively and efficiently recover required network or IT operations within the needed time frames.

Recommendation

We recommend that BSB assess its automated processing environment from a risk management and business continuity perspective and develop and test appropriate business continuity and contingency plans for IT systems under its charge. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to BSB's operations or the overall IT environment.

We further recommend that business continuity be tested and periodically reviewed and updated, as needed, to ensure the viability of the recovery plans. BSB's completed disaster recovery and contingency plans should be distributed to all appropriate staff, which in turn should be trained in the execution of the plans under emergency conditions. In addition, a complete copy of the plans should be stored in a secure off-site location.

Since BSB's mission is to help maintain state office buildings, it is recommended that BSB work in conjunction with the Division of Capital Asset Management to ensure that appropriate plans are in place

should one or more state buildings under BSB's charge become inoperable or inaccessible for a period of time.

We recommend that BSB's business continuity plans also identify the recovery strategies that its contracted vendors will follow in recovering the mission-critical HVAC system. The plans should also address recovery requirements and plans for any other essential systems.

Auditee's Response

In general we are comfortable with the findings in this document and agree that it provides us with some direction in strengthening systems within the Bureau that are IT related. To date BSB has accomplished the following with regard to documenting and strengthening our systems: We have initiated a planning process in collaboration with the Executive Office for Administration and Finance and the Information Technology Division with the intention of connecting vital building systems to separate and secure servers. This planning process was initiated in the summer of 2009. BSB is in the process of refining the scope of this project and identifying resources that would launch and maintain a secure network. BSB is in the process of reviewing its business continuity and recovery strategies with the intention of improving its policies and procedures and training staff.

Auditor's Reply

We commend BSB for initiating a planning process for connecting vital building systems to separate and secure servers. However, until disaster recovery and business continuity plans are developed and tested, BSB remains vulnerable to an interruption of service should an extended loss of IT capabilities occur.

2. Inventory Control over Computer Equipment

Our audit revealed that as of June 2008, the BSB neither maintained an inventory system of record for property and equipment nor performed an annual physical inventory and reconciliation of fixed assets for the fiscal year 2007. As a result, the BSB did not maintain an inventory record to properly account for the computer equipment that was under its charge. We also determined that BSB did not have a formal policy in place regarding the assignment and use of notebook computers. BSB had assigned four notebook computers to employees without requiring signed acceptance of the responsibility for security and authorized use.

During the course of our audit, the BSB developed an inventory listing of its computer equipment for fiscal year ending June 30, 2008. Our review of the BSB's initial inventory listing of computer equipment indicated that it did not contain all the asset information that is required by the Office of the State Comptroller. We examined BSB's June 30, 2008 IT inventory listing and found that although the record contained certain fields of information including location, description, and assigned employee, it lacked data fields such as cost and date of acquisition. Furthermore, other data fields containing information on serial number, tag number, BSB asset names, model, and manufacturer were incomplete.

Data regarding asset costs, tag numbers, and dates of acquisition are required by fixed assets regulations promulgated by the Office of the State Comptroller (OSC). Information regarding the status of an item supports IT configuration management by noting the asset's status, such as available for use, being repaired, obsolete, or designated for surplus.

Since the June 30, 2008 inventory record was not generated from sufficient supporting documentation of the IT equipment that had been purchased and disposed of, but rather was composed of a count of existing physical inventory, the inventory record could not be verified as accurate and complete. As a result, BSB could not provide reasonable assurance at that time of the integrity of the inventory record and the listing could not be relied upon to assist in the accounting for and verification of computer equipment. Furthermore, because of the lack of completeness of asset-related information, the inventory listing of computer equipment as of June 30, 2008 was insufficient to support BSB's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, meet IT configuration objectives, and serve as a reliable record of IT equipment.

We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is purchased, relocated, or disposed of. As a result, BSB could not provide reasonable assurance of the integrity of the inventory system of record for accounting for and monitoring computer equipment. Although BSB had developed an initial June 30, 2008 inventory of computer equipment, we determined that adequate procedures and control practices had not been implemented regarding maintenance and reconciliation of an inventory system of record for IT resources. Although fixed assets regulations promulgated by the OSC require the performance of an annual physical inventory of fixed assets, BSB senior management acknowledged that the first physical inventory of fixed assets of computer equipment was completed for fiscal year ending June 30, 2008.

During the audit, we provided guidance to BSB in creating an inventory listing that will serve as its official system of record for IT resources. Subsequently, we reviewed a revised IT inventory listing of July 31, 2008 that contained 108 computer equipment items. With respect to IT inventory recordkeeping, BSB senior management had recorded 96% of the BSB asset names and 93% of the model and manufacturer names on the revised IT inventory listing as of July 31, 2008. The other data fields of serial number and tag number remained incomplete. We also noted that the data fields for cost amount and date of acquisition remained unrecorded on the revised IT inventory listing.

Before the end of our audit, BSB further enhanced its inventory record for computer equipment. The updated inventory record obtained in November 2009 contained the data fields for cost and purchase date. We note that at that time BSB was in the process of making additional enhancements to its inventory

records. For example, equipment that had been leased was identified as such in the tag number column and other fields requiring further information had been highlighted or designated as "N/A."

Recommendation

To ensure that inventory control over IT resources is adequately maintained, we recommend that BSB strengthen documented inventory control procedures and practices to ensure compliance with policies and procedures required by the OSC's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and associated internal control documentation. Specifically, BSB should perform an annual physical inventory of computer equipment and reconciliation of the inventory system of record to ensure that an accurate, complete, valid, and current inventory record of IT resources is in place. IT equipment should be included in the inventory system of record for all fixed assets.

We also recommend that the inventory system of record be maintained on a perpetual basis and that it be periodically verified through reconciliation to physical inventory, acquisition, and disposal records. Furthermore, partially completed fields for serial number and tag number should be fully entered.

With respect to monitoring of the inventory record for computer equipment, BSB should improve documentation supporting the annual physical inventory, including a reconciliation of the physical inventory to BSB's inventory records. This improved documentation will help ensure the integrity of a perpetual inventory system of record for IT-related assets and provide reasonable assurance that BSB's inventory records can be effectively used to support IT configuration management and help safeguard computer equipment. Furthermore, we recommend that BSB maintain supporting documentation of the physical inventory performed and the reconciliation of physical counts and acquisition and disposal records to the perpetual inventory system of record.

With respect to notebook computers, we recommend that BSB develop a formal policy requiring that users who are assigned notebook computers must sign a responsibility and acceptable use form. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are exercised to reduce the risk of loss or misuse of the equipment. We recommend that BSB maintain a register of IT resources that have been signed out. The register should identify the item of equipment, the individual to whom the equipments was assigned, the date that the equipment was obtained by the individual, and the date when the equipment was returned.

Auditee's Response

In general we are comfortable with the findings in this document and agree that it provides us with some direction in strengthening systems within the Bureau that are IT related. To date BSB has accomplished the following with regard to documenting and strengthening our systems: BSB now has a formal policy in place regarding the assignment and use of notebook computers.

Auditor's Reply

While we acknowledge that BSB agrees with our audit results, we suggest that a plan of action be documented that addresses our recommendations regarding inventory control. We note that the inventory system of record should encompass all fixed assets along with the BSB's computer equipment.