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. 2010-0016-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AND RELATED ACTIVITIES AT THE MASSACHUSETTS EMERGENCY MANAGEMENT AGENCY

July 1, 2008 through April 23, 2010

OFFICIAL AUDIT REPORT

DECEMBER 20, 2010

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Emergency Management Agency (MEMA) was established under the Civil Defense Act, Chapter 639, of the Acts of 1950. Chapter 6A, Section 18, of the Massachusetts General Laws places MEMA within the Executive Office of Public Safety and Security (EOPSS). MEMA is responsible for coordinating federal, state, local, and private resources to protect the public during disasters and emergencies. MEMA's function is to develop plans for effective response to all forms of threat from natural or technological hazards, such as hurricanes, winter storms, floods, fires, hazardous material incidents, tornadoes, earthquakes, nuclear accidents, or terrorism. MEMA is also responsible for training emergency personnel to protect the public and themselves and assist individuals and communities in recovering emergency-related losses.

MEMA's resource network includes public health and safety officials; emergency workers; fire, police, public works, and transportation officials; nonprofit and volunteer agencies; private businesses and industry; and federal agencies. In addition to its headquarters in Framingham, MEMA has four regional offices of which Regions 1 and 2 are located in Tewksbury and Bridgewater, respectively. Regions 3 and 4 are located in Agawam. MEMA also has responsibility for the Radiological Instrumentation Maintenance and Calibration Facility (RIMC) located at the National Guard facility in Devens. At the time of our audit, MEMA employed 82 full-time equivalent (FTE) departmental staff.

MEMA's computer operations were configured in a local area network (LAN) supported by two file servers that connects through EOPSS Office of Technology and Information Services' (OTIS) file servers to the Commonwealth's state wide area network (WAN) to provide access to the Information Technology Division's (ITD) mainframes and file servers installed at the Massachusetts Information Technology Center (MITC). Through MEMA's LAN, access is provided to essential applications that reside on the OTIS file servers. The WAN provides access to the Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS). MEMA's essential applications include WebEOC that is used to manage information during and after an emergency event and the Electronic Comprehensive Emergency Management Plan (eCEMP) that enables communities to maintain emergency plans on an ongoing basis and provide MEMA with information about community resources. MEMA's other essential application is the Training Registration System (TRS) that enables the public to register for courses online and provides feedback (confirmation, reminders, directions, etc.) to course registrants.

With respect to network support functions at MEMA, there are two network engineers who are responsible for managing data files residing on the file server and for generating backup copies of

programs and data files onto magnetic media. OTIS has primary responsibility for management of the file servers, associated networks, and workstations located at MEMA's regional centers.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) audit at the Massachusetts Emergency Management Agency (MEMA) for the period covering July 1, 2008 through April 23, 2010. The audit was conducted from November 2, 2009 to April 23, 2010. Our audit scope included an examination of IT-related general controls pertaining to IT organization and management, logical access security, inventory control over computer equipment and wireless communication devices, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. In addition, our scope included a review of MEMA's control practices regarding Criminal Offender Record Information (CORI) checks for individuals hired or for employees being considered for promotion to positions having key responsibilities in fulfilling MEMA's mission. We also examined MEMA's controls over Personally Identifiable Information (PII) and its efforts to comply with the Commonwealth's data breach notification requirements.

Audit Objectives

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

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

Our objective regarding logical access security was to determine whether adequate controls were in effect to provide reasonable assurance that only authorized users were granted access to MEMA's application systems and whether password administration was actively being monitored. We also sought to determine whether the WebEOC, eCEMP, and TRS systems data was sufficiently protected against unauthorized disclosure, modification, or deletion.

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

With respect to the availability of the Executive Office of Public Safety and Security Office of Technology and Information Services (OTIS) computing system capabilities in support of MEMA's computer operations, we sought to determine whether disaster recovery strategies would provide reasonable assurance that mission-critical and essential IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible. In addition, we sought to determine whether adequate business continuity procedures were in place and in effect at MEMA including the generation and storage of on-site and off-site backup copies of magnetic media to support system and data recovery objectives.

Our audit sought to determine whether procedures were adequate for performing background checks on all individuals hired or promoted to positions that support MEMA's goals and objectives. We also sought to evaluate whether there were adequate controls in place to protect Personally Identifiable Information (PII) and to determine whether MEMA's control policies and procedures supported compliance with the Commonwealth's data breach notification requirements.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding OTIS and MEMA's overall mission and IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of activities and the internal control environment, we reviewed OTIS and MEMA's mission and primary business functions. In order to select areas to be reviewed, we performed a risk analysis of IT operations and selected applications. We assessed the strengths and weaknesses of the internal control system for selected IT activities, including organization and management, logical access security, inventory control over computer equipment and wireless communication devices, business continuity planning, and on-site and off-site storage of backup copies of magnetic media. We also reviewed control practices regarding CORI checks and MEMA's efforts to comply with PII standards and the Commonwealth's data breach notification requirements. Upon

completion of our pre-audit work, we determined the scope and objectives of the audit, and further developed our audit strategy.

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

To evaluate whether only authorized user access could be gained to MEMA's network and systems, we reviewed MEMA's logical access security policies and procedures with responsible security administrators. To determine whether logical access security controls were in place and in effect, we reviewed and verified the administration of logon IDs and passwords and selected control practices regarding logical access to network resources. To assess whether all users with active privileges were current employees, we obtained a list of individuals granted access privileges to e-mail accounts and other business-related applications, such as WebEOC, eCEMP, and TRS, and compared all users with active access privileges, as of January 19, 2010, to MEMA's list of current employees, including administrative and outsourced staff. To determine whether access privileges that were no longer required or authorized were disabled in a timely manner, we also compared the active network user listing to MEMA's listing of terminated employees and their respective termination dates. Furthermore, we reviewed password configuration and whether all persons authorized to access information system resources were required to periodically change their passwords and, if so, the frequency of the changes.

To determine whether MEMA complied with Commonwealth of Massachusetts regulations for fixed-asset accounting for equipment, we reviewed evidence-supporting performance of an annual physical inventory and reconciliation to the inventory records for computer equipment and wireless communication devices. To determine whether adequate controls were in place and in effect to properly account for MEMA's computer equipment and wireless communication devices, we reviewed inventory control policies and procedures and requested and obtained MEMA's inventory system of record for IT resources. We reviewed the inventory system of record as of October 26, 2010 for IT equipment installed at MEMA valued at $510,946 to determine whether the inventory contained appropriate data

fields to identify, describe, and indicate the value, location, and condition of the computer equipment and wireless devices. We also performed a data analysis on the inventory record of computer equipment and wireless devices to identify any unusual distribution characteristics, duplicate records, or unusual or missing data elements.

To determine whether the inventory system of record for computer equipment totaling $510,946 was current, accurate, complete, and valid, we used audit software to select a statistical sample of 55 (21%) desktops, monitors, printers and servers, with an associated value of $40,720 (18%) out of a total population of 267 items totaling $229,009. In addition, we selected a statistical sample of 26 (28%) laptops with an associated value of $50,147 (27%) from a total population of 94 laptops totaling $186,699. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory record to the actual computer equipment. To verify the relevance and completeness of MEMA's system of record for computer equipment, we selected 48 additional computer hardware items in adjacent locations to our original inventory sample and determined whether they were properly recorded on MEMA's inventory record. To confirm that the inventory system of record accurately recorded wireless mobile communication devices, we attempted to compare the carrier invoices for 60 mobile devices to the inventory list of IT resources.

To determine whether MEMA complied with Commonwealth of Massachusetts regulations for the disposition of surplus property, we reviewed records and supporting documentation for IT equipment disposed of during the audit period, as well as IT equipment that MEMA planned to request Commonwealth approval to dispose of as surplus. Finally, to determine whether MEMA was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we reviewed incident reports for missing or stolen IT equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

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

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

We interviewed senior management and reviewed MEMA's procedures and control practices to determine whether Criminal Offender Record Information (CORI) checks were performed prior to employment or for a change in position responsibility. To assess effectiveness and compliance with MEMA's policies and procedures pertaining to mandatory background checks, we reviewed 16 out of the total population of 82 MEMA employee personnel files and tested related documentation. We compared information outlined within Massachusetts General Law Chapter 6, Section 172 and 803 Code of Massachusetts Regulations (CMR) 3.05, Sections 1 and 2 with MEMA's CORI Request Form to our statistical sample of employees.

To determine the status of MEMA's compliance with respect to the handling of Personally Identifiable Information (PII), we reviewed Chapter 93H of the Massachusetts General Laws and Executive Order 504 to identify MEMA's responsibilities regarding protection of PII and notification for confidentiality breaches. With regard to the protection of personal information of MEMA's clients and staff, we interviewed senior management and reviewed MEMA's completed Self Audit Questionnaire (SAQ) and the Information Security Program (ISP) that includes an Electronic Security Plan (ESP).

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Criteria used in the audit included Chapter 93H of the Massachusetts General Laws; Executive Orders 490 and 504; Chapter 82 of the Acts of 2007; Chapter 647 of the Acts of 1989; management policies and procedures; and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Our audit of the Massachusetts Emergency Management Agency (MEMA) found that internal controls were in place to provide reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, on-site storage of backup copies of magnetic media, logical access security, Criminal Offender Record Information (CORI) checks, and protection of Personally Identifiable Information (PII). However, controls needed to be implemented or enhanced to provide reasonable assurance that the inventory system of record for IT resources is current, accurate, and complete and a comprehensive business continuity strategy and disaster recovery plan is in place to ensure that information system capabilities could be regained within an acceptable period of time. In addition, we found that MEMA needed to update its Internal Control Plan (ICP) to ensure that department-wide risks are identified and that policies, procedures, and controls are in place to mitigate those risks.

Our review of IT organization and management controls indicated that the Executive Office of Public Safety and Security Office of Technology and Information Services (OTIS), which supports MEMA's IT functions, had an appropriate and defined organizational structure and chain of command for the IT Department with assigned reporting responsibilities and documented job descriptions. OTIS also had documented IT strategic priorities that addressed MEMA's IT environment and the mission-critical WebEOC, Electronic Comprehensive Emergency Management Plan (eCEMP), and Training Registration System (TRS) applications.

Concerning internal control documentation, MEMA should update its Internal Control Plan, dated 2006, to help provide reasonable assurance that operational objectives are effectively and efficiently achieved and that undesired events are prevented or detected and corrected in a timely manner. Internal control documentation assists management in avoiding problems, such as overspending, operational failures, noncompliance with regulations, and violations of law. The annual update of the ICP will help ensure that risks are managed appropriately and assist MEMA in its efforts to implement a framework that mitigates identified risks by developing formally documented departmental policies and procedures, updating its business requirements, and defining management control objectives.

Regarding logical access security, we found there were adequate controls in place to restrict access to only authorized individuals within MEMA's local area network. Our audit revealed that MEMA had written IT procedures in place that provide for password creation/deletion, logon, and password configuration requirements. Our test of all 82 user ID's found that 100% were active employees. With regard to access security to mission critical applications used only during statewide emergencies, we found that MEMA had not updated user ID's assigned to approximately 1,200 individuals located throughout the 351 communities within the Commonwealth. MEMA should strengthen its logical access

security procedures by requiring outside users to reconfirm their logon ID's on an annual basis. Our test concerning access security for wireless mobile communication devices found that MEMA complies with Information Technology Division's (ITD) Enterprise Wireless Security Policy that includes Wireless Mobile Communications, Wireless Local Area Networks, and Wireless Wide Area Networks.

With regard to CORI, we found that controls were in place and in effect to provide reasonable assurance that MEMA is in compliance with Executive Order (EO) 495 regarding the use and dissemination of criminal record information. Further, we determined that personnel responsible for CORI have received the proper certification as required by the provisions of Chapter 6, Section 172, of the Massachusetts General Laws, pertaining to the dissemination of record information including certification, eligibility for access, scope of inquiry, and use of information. We also found that a CORI was conducted for all personnel and contractors that were included in our random sample of 16 employees (20%) hired or transferred into MEMA during the past two fiscal years. Although we found that procedural controls were in place, we determined that MEMA should develop documented policies and procedures for compliance with EO 495, Section 5 requiring that certified agencies maintain written policies regarding the use of CORI.

We determined from our analysis of security controls that MEMA has procedures in place to protect personally identifiable information from unauthorized disclosure that could potentially be used to uniquely identify, contact, or locate either employees or community users that access MEMA's mission-critical applications. In addition, we determined that MEMA has complied with Executive Order 504, Section 4 regarding the protection of information stored or maintained in electronic form by completing an information security plan (ISP), electronic security plan (ESP), and annual self-audit questionnaire (SAQ). We confirmed that a unique user ID and password are required to gain access to MEMA's local network and mission-critical WebEOC, eCEMP, and TRS applications. We determined that personally identifiable information is available internally to authorized users on a need-to-know and need-to-perform basis for data entry and/or read-only functions. Through our observations at MEMA, we verified that PII-related documents are shredded prior to disposal and offices and file cabinets containing PII were locked when not attended. We found that MEMA has provided reasonable assurance that it is complying with the guidelines set forth in Chapter 93H of the Massachusetts General Laws and EO 504. However, we determined that MEMA could enhance controls and mitigate risks associated with PII by developing documented policies and procedures based on generally accepted control practices.

Our review of business continuity planning indicated that although MEMA did not have a comprehensive business continuity strategy, a Continuity of Operation Plan (COOP), dated April 22, 2009, was in place, as well as other documented control practices encompassing an alternate relocation site and emergency notification plans. With respect to disaster recovery planning for computer operations, our audit

disclosed that MEMA did not have in place an approved, comprehensive, and tested disaster recovery plan (DRP) to restore computer operations in the event of a natural, manmade, or technological disaster. With regard to backup of magnetic media, we found that although backup copies for the mission-critical applications WebEOC and TRS are stored on-site in a fireproof safe, MEMA did not maintain off-site backup of magnetic media. We determined that under Executive Order 510 (EO 510), Enhancing the Efficiency and Effectiveness of the Executive Department's Information Technology Systems, that OTIS plans to assume operational responsibility for IT equipment and applications installed at MEMA effective fiscal year 2011. We determined that OTIS was in the process of developing a DRP that would apply to all 13 agencies within EOPSS, including MEMA, and that the DRP will also identify an alternate processing site. However, until OTIS, in conjunction with MEMA, develops, implements, and tests a comprehensive disaster recovery and business continuity strategy, MEMA remains at risk of being unable to recover computer operations and IT capabilities in a timely manner should a disaster occur.

Our audit disclosed that MEMA needed to improve inventory controls over computer equipment to ensure that the inventory record of IT resources is current, accurate, and complete and can be relied upon. We determined that MEMA's informal inventory procedures did not provide reasonable assurance that controls were in place to ensure that the inventory system of record for computer equipment, having a listed value of $510,946, is promptly updated when equipment is relocated, disposed of, lost, or stolen. We determined from our analysis of inventory records for the entire population of 486 IT computer-related items that information was missing or incomplete within data fields, including cost, acquisition date, purchase order, and description. We also found that the inventory system of record did not include wireless mobile communication devices that were assigned to MEMA personnel.

Regarding our test of the inventory system of record, our judgmental sample of 48 hardware items traced from multiple physical locations back to the inventory listing indicated that all of the selected items were on the inventory list. However, our test of 55 randomly sampled hardware items, totaling $40,720, tracing items from the official system of record to the items on the floor indicated that four pieces of computer equipment, totaling $2,388, could not be located. Furthermore, an inventory test of 26 laptop computers, totaling $50,147, indicated that four laptop computers, totaling $6,284, could not be found. Based on our examination of computer requisition forms associated with the 94 laptops listed on the inventory system of record, we found instances where laptops did not have a corresponding requisition form, forms were on file for laptops not on the inventory system of record, and forms were not signed acknowledging the return of laptops to the IT department. MEMA needs to improve inventory controls over IT resources to ensure the integrity of the inventory system of record.

AUDIT RESULTS

1. Disaster Recovery and Business Continuity Planning

We determined that although certain objectives for contingency planning existed, MEMA did not have in place a documented disaster recovery plan (DRP) and business continuity plan (BCP) or provisions for off-site storage of backup copies of magnetic media in place to provide for the timely restoration of business and computer capability functions should MEMA's IT systems be rendered inoperable or inaccessible. We determined that MEMA had a Continuity of Operation Plan (COOP), dated April 22, 2009, that focused on restoring MEMA's essential business functions at an alternate relocation site and performing those functions before returning to normal operations. However, by not having a formal DRP and user area plans in place that work in conjunction with the COOP, MEMA is at risk of being unable to address a catastrophic event that would deny access to its facility or render its IT capabilities inoperable for an extended period of time.

We determined that under Executive Order 510, the Executive Office of Public Safety and Security's Office of Technology and Information Services (OTIS) plans to assume operational control of MEMA's IT operations effective fiscal year 2011. We determined that OTIS is in the process of developing an enterprise-wide DRP that will include IT operations at MEMA. In the interim, OTIS is developing plans to utilize IT equipment at the State Police General Headquarters located in Framingham as an alternate processing site until fiscal year 2012, at which time the Springfield Data Center will be designated as the alternate processing site for MEMA's network and mission-critical applications. The completion of documented plans for the use of an alternate processing site will allow OTIS/MEMA the flexibility to restore network capabilities for an extended period of time at an alternate location in order to gain access to its mission-critical WebEOC, TRS, and eCEMP applications The WebEOC and TRS applications, which reside on a server located at MEMA's Framingham location, will eventually transition to the OTIS server located in Chelsea. The eCEMP application has been transitioned to the OTIS server located in Chelsea where weekly backup of magnetic media is stored in a secure location. The absence of formally documented contingency plans to address disaster recovery places at risk MEMA's ability to ensure that systems are recovered to provide access to mission-critical IT applications in the event of a natural catastrophe (i.e., tornado, flood, wind damage, hurricane, fire), man-made disaster (i.e., terrorism, blackouts), or technology-based event (i.e. cyber attack).

Although MEMA understands that IT systems may need to be recovered under disaster scenarios, an appropriate risk analysis methodology was not conducted to identify the relevant threats that could render IT systems inoperable or inaccessible, the likelihood of the threat, and the expected frequency of

occurrence for each disaster scenario. As a result, if a disaster were to occur, MEMA may not have sufficiently developed recovery strategies and the foundation and structural framework for managing computer capabilities associated with emergency response and continuity of responsibilities to support MEMA's mission within an acceptable time period.

We determined from our review of the COOP that MEMA had associated control practices in place, including identification of emergency relocation groups (ERG), an emergency relocation site (ERS), and agency critical systems. While MEMA management had assessed the relative criticality of its computing systems and developed various policies, we found that MEMA had not outlined or tested a comprehensive approach to ensure continuity of essential services in the event of a disaster. If a disaster were to occur, there are no contingency plans developed by departments to address critical business functions throughout MEMA. By necessity, the BCP includes planning for contingencies inclusive of disaster recovery and would be focused on the information system functions that are the most necessary to continue agency operations at a departmental level.

An up-to-date effective BCP should identify the manner in which essential services would be restored or replaced without the full use of the data center facility or loss of network communications. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical computer processing functions, either at the original site or at an alternate processing site. MEMA should include in the BCP risk assessment information that identifies the relevant threats that could significantly impact computing capabilities associated with business functions, the likelihood of the threat, and frequency of occurrence for each disaster scenario. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the alternate site being used for restoration efforts.

With regard to backup of magnetic media, we found that MEMA generates and stores in a fireproof safe daily and weekly backup copies of network and mission-critical data. However, we determined that MEMA does not maintain off-site backup of magnetic media. The development and implementation of a comprehensive BCP and DRP strategy should include provisions for the off-site storage of backup copies of systems and data files that can be accessed by only authorized personnel and used in a secure manner to recover IT operations to support essential business processes.

Recommendation

We recommend that MEMA work closely with OTIS during the consolidation and transition of IT operations to detail disaster recovery and business continuity plans that incorporate criticality and impact

assessments, risk management, recovery plan testing and maintenance, recovery procedures, training, and communication. In addition, a security risk assessment of recovery plans should be completed on an annual basis, or upon major changes to IT or business operations, to assist in ensuring the applicability and readiness to address current business objectives. To help ensure that MEMA reacts optimally in the event of a disaster, the DRP and user area plans should be developed to work in conjunction with MEMA's COOP detailing MEMA's current mission-critical operations, applications, and supporting IT infrastructure and a risk analysis assessment of various disaster scenarios. The DRP should also address IT recovery under circumstances when access to MEMA's facility is denied for an extended period of time. The DRP should be an IT-focused plan that includes restoring information systems operability and IT capabilities at an alternate processing site. In this regard, OTIS should expedite its plans to utilize the State Police General Headquarters as an alternate processing site and storage of backup media to assist in ensuring continuity of IT operations in the event that MEMA's computer operations are rendered inoperable.

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

MEMA should establish a business continuity planning framework that incorporates criticality and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training, and communication. MEMA should work in partnership with OTIS to develop and implement a cohesive business continuity and contingency plan that includes disaster recovery planning and works in conjunction with the COOP to mitigate the disruption to its computing capabilities and/or business operations should a disaster occur. In addition, MEMA's business continuity plan should document vendor protocol for the emergency use of computers suitable for operating its mission-critical applications, include provisions for periodic training for the staff, and ensure that a complete hard copy and electronic copy of the plan is stored in a secure off-site location.

Auditee's Response

MEMA along with the rest of the Executive Office of Public Safety and Security (EOPSS) is undergoing a process of Information Technology consolidation. This consolidation will result in all of our systems being managed by staff from the Office of Technology and Information Services (OTIS). MEMA, as an agency, will no longer be responsible for system and user equipment repair, inventory control or procurement of IT equipment. MEMA and OTIS are aware that a comprehensive business continuity and disaster recovery plan must be developed according to best practices and in a timely fashion. Both agencies recognize that such planning is necessary to ensure that their business processes and delivery of services can be maintained in the event of a catastrophic hardware failure or data loss. While MEMA has policies and procedures that form the basis of a business continuity plan and OTIS has policies and procedures that were developed during its former charter as Criminal History Systems Board (CHSB) for disaster recovery, (and the construction of a secondary offsite fallback data center is being planned in Western Massachusetts), such materials need to be merged into a comprehensive business and disaster recovery plan to guide both agencies should a disaster strike. The Director of MEMA and the [Secretariat Chief Information Officer] SCIO for EOPSS will be developing the necessary goals for comprehensive business continuity and disaster recovery planning and recognize that business continuity and disaster recovery planning must factor in the specific business needs of each operation and that it should not focus solely on the restoration of IT equipment.

For the purposes of continuity planning, MEMA has listed these systems in the MEMA COOP plan and has identified them as "dependant" upon outside services, namely OTIS. Each COOP plan template has a section for these identified dependencies that include vendor contracts, commercial services, maintenance contracts and utility infrastructure. The Statewide Continuity Program, which MEMA oversees, has recommended that Secretariats treat their IT divisions as separate agencies for COOP planning purposes, each with their own Essential Functions and Critical Systems, as has been done in EOPSS.

Auditor's Reply

We are pleased that EOPSS, in conjunction with MEMA, recognized the need for a comprehensive approach to disaster recovery and business continuity planning. As IT consolidation evolves and responsibilities increase for OTIS, we suggest that a risk assessment of IT capabilities for MEMA be performed and updated as the IT and operational environments change.

2. Inventory Control over Computer Equipment

Our audit disclosed that MEMA's inventory controls over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in MEMA'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 inventory record of computer equipment was being maintained on a perpetual basis. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is acquired, relocated, disposed of, or lost. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an

appropriate level of reconciliation was not in place. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured.

We determined that MEMA had informal procedures regarding the purchasing and receiving of IT resources. However, we found that MEMA needed to develop documented policies and procedures regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. We determined that MEMA was not in compliance with the reporting of lost or stolen equipment per Chapter 647 of the Acts of 1989 and disposal of surplus property in compliance with 802 Code of Massachusetts Regulations (CMR) 3.00 as MEMA failed to submit required notifications to the Office of the State Auditor and the State Surplus Property Officer, respectively. Specifically, during our review of lost or stolen equipment, we noted that one laptop was reported missing to the Taunton Police Department. However, the missing laptop was not reported to the Office of the State Auditor in accordance with Chapter 647 of the Acts of 1989. We also observed during our testing that MEMA had designated certain IT equipment as surplus, but had not properly identified the items on the inventory system of record or provided the State Surplus Property Officer with an accurate accounting of surplus items.

With respect to the recording of IT-related assets, we found that MEMA lacked appropriate and adequate management oversight to prevent and detect errors in the recording of identifying data for computer equipment entered into MEMA's inventory system of record. Our analysis of MEMA's inventory system of record indicated that most required data fields, including barcode, item description, manufacturer, model, serial number, and location were present. However, based on our test of 16 data fields consisting of 486 items, we determined there was a significant amount of information missing from certain data fields including cost (31%), date received (34%), encumbrance number (43%), and assigned to (76%). Although MEMA provided an inventory system of record that listed IT-related assets as of October 26, 2009, we were unable to determine the total value of the inventory because the cost was not recorded in data fields associated with 31% of the items. By failing to record the historical cost of purchased computer hardware items and date received on MEMA's inventory system of record, MEMA was not in compliance with the joint policy of the Office of the Comptroller (OSC) and Operational Services Division (OSD) dated July 1, 2004, revised November 1, 2006.

Our inventory tests of MEMA's inventory system of record were conducted against a total population of 486 IT-related assets with an associated value of $510,946. To verify the integrity and completeness of the inventory system of record, we judgmentally selected 48 items totaling $27,810 in adjacent locations to our statistical sample of 55 items consisting of desktops, monitors, and printers. Our test found that

100% of the 48 judgmentally selected items on the floor were properly identified on the IT inventory system of record. To further verify the items listed on the inventory system of record, we inspected the existence and the recorded location of our statistical sample of 55 items valued at $40,720. We determined that 51, or 93%, of the 55 items were properly identified on MEMA's listing of inventory computer equipment. However, based on our testing, we determined that four items consisting of one desktop, two monitors, and one printer with an aggregate value of $2,388 representing a 7% error rate were not at the locations indicated on the inventory system of record. We also selected a statistical sample of 26 (27%) laptops totaling $50,147 out of a total population of 94 laptops totaling $186,699 and found that the location of four (15%) of the laptop computers tested, valued at $6,284, could not be verified. Missing laptop computers containing sensitive data could present a potential risk to MEMA's proprietary data and personally identifiable information.

During our analysis of inventory controls, we found that wireless mobile communication (WMC) devices were not included on the inventory system of record. We determined that MEMA's 60 WMC devices consisting of 23 Blackberry's, 12 Nextel devices, 15 AT&T devices, and 10 satellite phones were recorded on three lists maintained by two departments. Based on our comparison of the listings of WMC devices to invoices from their respective carriers, we found that six devices billed by Sprint and the 15 AT&T devices were not included on any listing. Based on our comparison of the individuals assigned a WMC device to MEMA's list of active personnel, we determined that one of the six devices not included on any listing was assigned to a terminated employee. We noted that MEMA notified the carrier to discontinue service, but that the carrier had not removed the item from the monthly bill. MEMA subsequently requested the appropriate credit for charges.

We determined that MEMA maintained a policy of obtaining a computer requisition form (CRF) signed by a user to acknowledge receipt of a laptop computer. However, we found that of the 94 laptops identified on the inventory system of record, 30 or 32%, did not have an associated CRF. In addition, we found that 26 CRF's were for laptops not included on the inventory system of record. We determined that of the 120 CRF's reviewed by the audit team, 27, or 23%, indicated laptops were signed out for a specified period of time but did not have an authorized signature to indicate their return. We also observed that MEMA signed-out multiple laptops on one form thereby increasing the risk that individual laptops may not be properly recorded on the inventory database. Based on our test results, the CRF's used for the loan of computer equipment lacked the necessary controls needed to accurately record laptop computers on the inventory system of record As a result, there is an increased risk that laptop computers that contain proprietary data and personally identifiable information may be lost or stolen.

Recommendation

To ensure that inventory of IT resources is adequately maintained, we recommend that MEMA strengthen current practices by developing documented policies and procedures that are in compliance with requirements set forth in the joint policy of the Office of the Comptroller (OSC) and Operational Services Division (OSD) dated July 1, 2004, revised November 1, 2006. Procedures to support MEMA's policies should be documented, implemented, and monitored to help ensure that equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of equipment.

MEMA should provide the Office of the State Auditor (OSA) with information regarding the laptop that was reported missing to the Taunton Police Department and ensure that procedures are in place for the immediate reporting of lost or stolen equipment as required by Chapter 647 of the Acts of 1989. If MEMA cannot locate the missing computer equipment identified during our testing, MEMA should also report these items to the OSA. MEMA should also determine whether the four laptops and one desktop computer contain any proprietary or personally identifiable information and take appropriate action to mitigate any related risks.

We recommend that items that have been deemed as surplus or obsolete property, traded in for new equipment, or donated should be assigned the appropriate condition code on the master inventory listing. MEMA should then compile a listing of all surplus equipment, complete Form OSD 25 **(**Declaration of Surplus Property), and forward the required documentation to the State Surplus Property Officer.

With respect to IT configuration management and the integrity of the inventory system of record, MEMA should update missing information in its inventory data fields with specific attention to cost, date received, encumbrance number, and to whom the equipment is assigned. In addition, MEMA's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

In order to ensure safeguarding of laptops and to minimize the risk of lost or stolen equipment, we recommend that MEMA strengthen its controls to maintain complete and up-to-date signed computer requisition forms to record that users have received or returned their laptops. MEMA should implement controls to ensure that a computer requisition form is required for the sign-out of each laptop rather than having multiple laptops signed out on one form.

We recommend that MEMA implement controls to consolidate the recording of all wireless mobile communication devices into the inventory system of record in lieu of maintaining separate lists by

multiple departments. MEMA should also ensure that documented procedures are in place to periodically match mobile carrier invoices to the active personnel list to ensure that billings are discontinued for terminated or transferred employees.

The strengthening of asset management controls will help to improve the integrity of MEMA's inventory system of record and allow MEMA to properly account for computer equipment, evaluate the allocation of equipment, identify missing equipment, promptly report lost or stolen items, and meet IT configuration objectives.

Auditee's Response

This audit, 2010-0016-4T, itself served as an excellent reference point for improvements to our policies and procedures regarding the current IT inventory. With the IT consolidation taking place throughout EOPSS, OTIS is working diligently with all agencies to review their processes and procedures and to ensure that there are no gaps with regards to the handling of IT assets. MEMA will continue to work with OTIS to review and develop appropriate controls for all IT property used throughout the agency.

MEMA, through the CFO, will report to the Office of the State Auditor, MEMA's Agency Head, and the EOPSS Secretariat Chief Information Officer (SCIO) regarding the laptop that was reported missing to the Taunton Police Department, as required by Chapter 647 of the Acts of 1989. It should be noted that this incident occurred during a previous MEMA administration. MEMA's current Acting Director, appointed in June 2010, is actively engaging with MEMA's Executive Staff to establish appropriate and necessary policies governing the agency's operations. This will include a policy that requires immediate reporting of lost or stolen equipment, as well as a procedure of notification that complies with the requirements of Chapter 647 of the Acts of 1989. MEMA will continue to investigate the location of the 5 computers identified as missing during the audit testing, and if unable to locate them, will also report these losses to the Office of the State Auditor, MEMA's Agency Head, and the EOPSS Secretariat Chief Information Officer (SCIO). MEMA's Information Security Officer will determine whether these computers contain any proprietary or personally identifiable information and take appropriate action, if needed.

MEMA concurs with the findings concerning its inventory system of record. MEMA conducted a full and complete physical inventory for the State fiscal year ended June 30, 2009. However, as noted in this audit report, its current software does not adequately record all data element fields as required by state policies or federal regulations. Much of the missing information occurred during a failure of the software system in 2008. Some of the corrupted information fields carried forward when the database was rebuilt. MEMA will evaluate available inventory software and work in collaboration with OTIS to develop a robust and capable application for recording inventory. This new system shall include a controlled data collection process to safeguard the integrity of the data. It is anticipated that this project will begin within the current fiscal year.

During its most recent physical inventory, MEMA identified many IT assets that are either surplus or obsolete for the State fiscal year ended June 30, 2009. However, the effort to properly dispose of these has stalled. MEMA will continue the process to dispose of these assets in accordance with the policy of the Operational Services Division regarding

surplus property. MEMA will update its current inventory system of record as these items are resolved, including making proper notification to the State Surplus Property Officer, MEMA's Agency Head, and the EOPSS SCIO.

MEMA concurs with the findings concerning adequate controls over the requisition of IT equipment. As the IT Consolidation moves forward, it is anticipated that all existing IT assets will be transferred to OTIS. As of July 1, 2010, all IT equipment purchases are made by EOPSS-OTIS and the assets and inventory will be owned and managed by OTIS. It is anticipated that a controlled requisition process will be determined to the mutual benefit of both organizations.

MEMA does not typically record wireless mobile communication devices in its inventory system of record. These items do not meet the threshold for inventory reporting or control as set forth in the joint policy of the Office of the Comptroller and Operational Services Division. MEMA currently matches mobile carrier invoices to the active personnel list on a quarterly basis, ensuring service termination and equipment transfers are accurate. MEMA also reviews each invoice monthly to identify any incorrect or inappropriate charges. MEMA asserts that these procedures provide adequate assurance that its wireless mobile communications devices are used for their approved purposes and maintained and accounted for appropriately.

Auditor's Reply

We commend the actions initiated by MEMA and OTIS to improve fixed-asset inventory controls. We believe a single comprehensive inventory control system for all MEMA fixed assets is an important element for an overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding fixed assets and assist IT infrastructure and configuration management decisions.

Updating the inventory record when changes in status or location occur will strengthen the accounting of fixed assets. An updated perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for any lost, stolen, or surplused equipment. In addition, these efforts should help minimize the risk of lost or stolen equipment and improve the identification of the status of equipment for configuration management purposes.

Although wireless communication devices do not meet the threshold as set forth in the joint policy of the Office of the State Comptroller and Operational Services Division, we note that MEMA, in keeping with best practices, includes in its inventory system of record telecommunication devices and computer equipment that are below the threshold. Best practices with regard to configuration management also require that IT-related assets including those that connect to the network are managed within a centralized inventory system. Asset tracking and monitoring of wireless communication devices will help to ensure compliance with security standards and prevent theft, misuse, and abuse.

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

3. Internal Control Plan

Our audit disclosed that MEMA's internal control plan, dated February 2006, had not been updated annually as required by Chapter 647 of the Acts of 1989, An Act Relative to Improving Internal Controls within State Agencies. Chapter 647 establishes the minimum level of quality acceptable for an internal control system in operation throughout Commonwealth agencies and departments. We found that MEMA had not conducted a current review and comprehensive assessment of risks that could impede the attainment of department goals and objectives. By not conducting an annual update of its internal control plan, MEMA had not required staff to identify and implement policies and procedures to mitigate risks, especially those related to the prevention of fraud, waste, and abuse. An updated internal control plan will assist management in achieving operational objectives, such as ensuring that best practices are in place for the reporting of funds associated with federal grants. An annual update of the internal control plan will also assist MEMA in optimizing its efforts in ensuring the integrity, security, and availability of MEMA's systems and records, and in protecting and effectively using its resources.

The absence of an updated internal control plan limits MEMA's ability to ensure that control practices are in place to mitigate risks associated with MEMA's mission, goals, and objectives. We note that when MEMA completed its annual internal control questionnaire, it recognized the need to update its internal control plan and ensure that departmental policies and procedures are in place as required by Chapter 647. An updated internal control plan would strengthen MEMA's framework of control and address the control requirements set forth by Chapter 647 and the Office of the State Comptroller.

Recommendation

We recommend that the MEMA's Internal Control Officer work with MEMA's various departments to identify and document operational and control objectives and risks, and identify and update existing control policies, procedures, and management control practices. We recommend that the process of completing the internal control plan include identifying any gaps in required controls and developing a plan to design, implement, and exercise any additional controls required. Lastly, we recommend that

MEMA's internal control plan ensure compliance with the Office of the State Comptroller's internal control guidelines that include monitoring grants and the prevention of fraud, waste, and abuse.

Auditee's Response

MEMA concurs with the finding concerning its outdated Internal Control Plan. MEMA's Acting Director and Executive Staff will work collaboratively to assess the agency's risks and establish appropriate controls to mitigate them. A comprehensive review of the agency's business processes and associated procedures is currently underway as the agency upgrades its technology components and capabilities. As the review progresses, MEMA's Internal Control Officer will work with Agency staff and OTIS to perform an enterprise risk assessment of its IT-related products and functions. MEMA proposes to train its key staff members in the development of internal controls and the prevention of fraud, waste and abuse. The Office of the State Comptroller offers an extensive program that is available to all employees. MEMA will work to develop its Internal Control Framework in consideration of all programmatic and functional responsibilities of the Agency. It is anticipated that a revised and more robust ICP, articulated to and supported by agency personnel, will be under development throughout FY2011.

Auditor's Reply

We are pleased that MEMA plans to update its internal control plan to ensure compliance with Chapter 647 of the Acts of 1989 and the Office of the State Comptroller's guidelines.