A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

NO. 2003-1370-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE OFFICE FOR REFUGEES AND IMMIGRANTS

JULY 1, 2002 through APRIL 25, 2003

OFFICIAL AUDIT REPORT
DECEMBER 16, 2003

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Office for Refugees and Immigrants (ORI) was created in 1985 as the Massachusetts Office of Refugee Resettlement charged with administering the state's refugee resettlement program under the federal Refugee Act of 1980. M.G.L. Chapter 6, Section 207 outlines the powers and duties of the Office for Refugees and Immigrants. The Office's mission was expanded and its name was changed in 1986 after passage of the Federal Immigration Reform and Control Act (IRCA). Among its many provisions, the IRCA created a onetime amnesty program for individuals who were living in the United States illegally. Following IRCA, ORI expanded services to individuals from a wide variety of countries of origin who were not classified as refugees.

The ORI's mission statement is to support the effective resettlement of refugees and immigrants in Massachusetts; promote the full participation of these new Americans in the economic, civic, social, and cultural life of the Commonwealth; and foster a public environment that recognizes and supports the ethnic and cultural diversity of the state. The ORI's web page provides information about the Office's four business units, the Community Building, Family Independence, Fiscal, and Contract. "The needs of Massachusetts refugees and immigrants continue well beyond their first 18 months of resettlement in the United States. As individuals and families begin to establish self-sufficiency in their new home, they often need assistance in developing the capacity to ensure the immediate and long-term well-being of their communities. ORI assists community development efforts through a variety of programs and special projects administered through the Community-Building Unit. This includes support for the establishment and strengthening of self-help organizations, provision of services for youth and older refugees, programs which provide assistance with the process of becoming an American citizen, and special projects which address organizational capacity-building and existing gaps in services."

Through the Family Independence Unit, ORI administers the Massachusetts Refugee Resettlement Program (MRRP) with ORI's federal funding source, the Office for Refugees and Resettlement (ORR). The unit must carry out all necessary procurement activities, and distribute and account for the Refugee Cash, Medical Assistance and support services funds provided for refugee resettlement in Massachusetts. The Family Independence Unit also applies for and administers Targeted Assistance Discretionary and Formula Grants. These grants are allocated to states by ORR to

provide employment training for certain refugees with multiple barriers to employment, help refugee women overcome cultural barriers to employment, help former political prisoners gain employable skills, and to fund employment and other services in certain local areas with large refugee populations. The Family Independence Unit reports regularly to ORR on the progress of MRRP, and the expenditure of funds. It provides the federal agency with a continuing analysis of the refugee picture in Massachusetts.

The ORI Fiscal Unit is responsible for managing the financial control functions necessary to enable the agency to operate its programs effectively and efficiently in compliance with recognized standards for the use of public funds. These functions include accounting, budgeting, federal revenue management, financial reporting and recording, auditing, financial analysis, cost evaluation, and examinations of related federal and state fiscal regulations. On a day-to-day basis, the Fiscal Unit staff process all agency payments including the payment of individual transitional assistance benefit checks to refugee clients. The unit staff work closely with ORI program and contract staff, providers and vendors, and the staff of the offices of the State Treasurer, Comptroller, Fiscal Affairs Division, and Purchasing Agent. ORI Fiscal Unit staff also work with staff of the federal Health and Human Services Division of Grants Management and Division of Payment Management.

The Contracts Unit oversees ORI's responsibilities to the Commonwealth of Massachusetts governing procurement policies and procedures. This is inclusive of commodities and human and social services requiring competitive procurements, vendor review and selection, contract negotiation and execution, and compliance monitoring of terms and conditions to ORI contracts. During any given fiscal year, the Contracts Unit staff oversee one hundred to one hundred fifty plus contracts, each of which would range from $5,000 to $500,000. Since most ORI funds are federal, a dual accountability to federal regulations and state regulations exists.

The ORI's office is located at 18 Tremont Street, Boston, Massachusetts. The ORI reports to and is funded by the Executive Office of Health and Human Services. During fiscal year 2002, grants administered by ORI totaled $6,562,709. At the time of our audit, the ORI information technology (IT) facilities were connected through the Commonwealth's wide area network to the Administration and Finance's Information Technology Division's (ITD) data center for access to the Massachusetts Management Accounting and Reporting System (MMARS), which is the

Commonwealth's centralized accounting information system, and to the Human Resources/Compensation Management System (HR/CMS).

The IT infrastructure at ORI consists of two networked file servers and 24 desktop computers. The ORI relies on Microsoft Office Suite products to support its business activities. In addition, ORI has implemented Mass Mail, which is an ITD-supported centralized e-mail system utilizing Windows 2000, and Microsoft Outlook. The ORI is attempting to develop a networked system called Massachusetts Office for Refugees and Immigrants (MORI) in an effort to enhance their current system to gather statistical information to improve state and federal reports.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope:

Our audit, which was conducted from October 4, 2002 through April 25, 2003, consisted of an examination of selected IT-related areas at the Office for Refugees and Immigrants (ORI) covering the period of July 1, 2002 through April 25, 2003. Our audit scope consisted of an examination of IT-related controls pertaining to organization and management, physical security, environmental protection, hardware and software inventory, system access security, business continuity and contingency planning, and on-site and off-site storage of backup copies of magnetic media.

Audit Objectives:

The primary objective of our audit was to determine whether adequate controls were in place and in effect for selected IT-related areas. We sought to determine whether the Office's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be achieved to support business functions. We further sought to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the office area, file server room, and on-site and off-site storage areas for backup magnetic media were limited to only authorized personnel. Moreover, we sought to determine whether sufficient environmental protection was being provided to prevent and detect damage or loss of IT-related equipment and media.

We evaluated whether an effective business continuity and contingency plan had been implemented to provide reasonable assurance that IT operations could be regained within an acceptable period should a disaster cause computerized operations to fail, or for systems to become inaccessible. We also sought to determine whether adequate controls were in place to ensure that backup copies of all mission-critical and essential media were being generated on a regular basis and whether they were properly labeled and accounted for. In addition, we sought to determine whether copies of backup media were stored in secure on-site and off-site locations to enable a controlled restoration of the system and data files should a disaster require recovery efforts.

We sought to determine whether adequate system access security controls were in place to provide reasonable assurance that only authorized users would have access to the Office for Refugees and

Immigrants' automated systems. We evaluated whether adequate controls were in place to prevent unauthorized access to data and systems and whether IT management was notified when users terminated employment or when there was a change in job functions that would alter the user's access privileges.

With regard to fixed-asset management, we evaluated whether hardware and software were safeguarded from unauthorized use or theft, whether the hardware assets were accurately reflected in the fixed asset inventory and accounting records, and whether an annual physical inventory was conducted. We also sought to determine whether copies of software licenses were on file for microcomputer and LAN-based software.

We performed a review of ORI's proposed client tracking system. This system, when completed, will enhance the office's current system to gather statistical information for improved state and federal reports.

Audit Methodology

As part of our pre-audit work, to determine areas to be examined for our audit scope and objectives, we met with ORI senior management to discuss current IT-related operations; reviewed documentation regarding the mission, organization, and management of ORI; and conducted a pre-audit survey. We identified IT-related equipment and their location and conducted a preliminary review of the file server room. We also performed a high-level risk analysis and conducted a preliminary review of controls.

Regarding our review of organization and management, we interviewed senior management, reviewed and analyzed documentation (policies and procedures for IT, security procedures, organization chart, IT job description, risk assessment memorandum, network configuration, and the business continuity and contingency plan) provided, and assessed IT-related management practices.

To assess physical security and environmental protection, we interviewed management and inspected the room housing the file server and on-site storage of backup media, the general office area, and the off-site storage area for backup copies of magnetic media. We reviewed sign-in/sign-out procedures, escorting of visitors, parameter security for locked doors and windows, and general

building security. We reviewed the Office's record keeping for individuals provided with keys and determined whether keys were issued to only current staff members. For environmental protection we reviewed fire prevention and detection, fire suppression, general housekeeping, temperature control, and uninterruptible power supply.

To determine whether system access security controls were in place to provide reasonable assurance that only authorized users would have access to programs and data files, we obtained and reviewed system access security policies and procedures and conducted selected tests. To determine whether user IDs and password security were being properly maintained, we interviewed the security administrator and assessed the level of access security being provided. To determine whether only authorized access privileges existed on the system, we reviewed procedures for granting system access. In addition, we compared and verified the system-generated list of staff authorized to access the automated systems to the list of current ORI employees.

To evaluate whether the Office's hardware and software inventories were properly accounted for and controlled, we sought to obtain their documented inventory control policies and procedures and a copy of the inventory record. We reviewed the inventory systems record layout for the appropriateness and comprehensiveness of required information. We assessed the adequacy of inventory controls by testing the integrity of the inventory record, determining whether equipment was properly tagged with ORI identification numbers, and determining whether annual inventory reconciliations were performed. To determine whether inventory records were current, accurate, and valid, we tested all hardware items listed on the inventory record and compared them to their physical locations. In addition, we traced all items from their physical locations to the inventory record. We also obtained an inventory for software licenses for microcomputer and LAN-based software. In addition, we reviewed ORI's procedures for the reporting of lost or stolen property.

To assess the adequacy of business continuity and contingency planning, we interviewed management and determined whether a formal, written and tested business continuity and contingency plan had been developed to resume computer operations should the Office's LAN and microcomputer systems be rendered inoperable. Concerning off-site storage of backup media, we inspected the off-site location and verified that backup copies of magnetic media were stored there. We also determined whether the criticality of application systems had been assessed and whether risks and exposures to computer operations had been evaluated.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted auditing practices. Audit criteria used in the audit included management control practices outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based upon our examination of internal controls at the Office for Refugees and Immigrants (ORI), we found that controls were in place to provide reasonable assurance that IT resources would be properly recorded and accounted for on the Office's inventory system of record and that only authorized users had access to the Office's systems. We found that although overall organization and management controls provided reasonable assurance that an appropriate organizational structure was in place and that responsibilities and reporting lines were defined, IT-related policies and procedures needed to be enhanced to adequately address environmental protection, hardware and software inventory, and business continuity and contingency planning. Our review of organization and management confirmed that ORI's organizational controls included an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for information technology staff. Overall, ORI management was aware of the importance of having appropriate internal controls in place.

Adequate internal controls were in place to provide reasonable assurance that physical security and environmental protection control objectives would be met, except for the file server room. We found that appropriate air quality in terms of temperature was not being afforded on a continual basis, often requiring that the door to the file server room be left open. In the absence of sufficient air conditioning for the file server room, a fan was used in conjunction with leaving the door open to help circulate the air and improve general ventilation. Because the room is accessible by the general public, it is important that an appropriate level of security be in effect to reduce the risk of unauthorized access. As a result, none of the IT resources, including backup copies of magnetic media stored on site, was sufficiently secure on a continual basis.

Our review of system access security controls revealed that only authorized users had access to the Office's local area network (LAN). We found that appropriate logon procedures were in place to gain access to system resources. In addition, appropriate control practices for password composition, length and frequency of required change were in place. Regarding the latter, passwords would expire upon reaching a pre-set number of days, and users were required to enter a new password to continue having system access. Although there was an adequate understanding of the procedures to be followed to activate or deactivate a user account, associated policies and procedures were not sufficiently documented. For example, there were no formal, written policies

or procedures to activate and deactivate user accounts from the LAN in a timely manner. Regarding password composition, passwords were case sensitive, and required a minimum of eight characters comprising of an uppercase and lowercase character, numeric and/or special character. Moreover, users could not use part of their full name or the @ symbol in their passwords.

Controls needed to be strengthened to increase the likelihood that IT resources would be properly recorded and accounted for on the Office's inventory system of record. Although the Office maintained a perpetual inventory of all equipment, including hardware and software, and the inventory had appropriate data fields to properly identify the recorded items, the inventory was not being monitored and reconciled on a frequent enough basis to ensure adequate data integrity. Our audit tests indicated that all 26 microcomputer workstations could be traced from their physical location to the inventory record, however, the two file servers located at the ORI's file server room were not listed on the inventory record. Our review of the overall inventory record also indicated that it listed all types of equipment that had been purchased since March 1, 1988. As a result, the list overstated the number of items and total value, because the list included equipment that has been surplused. For example, the inventory included 364 items of IT equipment that had been surplused and were no longer at the agency. We also found that there were a limited number of duplicate records for surplused equipment. During the course of the audit, the ORI corrected these deficiencies. In addition, a software inventory was also obtained.

We determined that the Office did not have a formal, written, or tested business continuity and contingency plan to provide for timely restoration of essential business functions should systems processed through ORI's LAN be rendered inoperable or inaccessible. If automated systems under ORI's control were unavailable, or if the current systems and business office could not be accessed, the ORI should have a plan in place to restore a designated level of required services within a predefined time period at another processing site. The plan would include IT restoration to the extent needed. We found that appropriate on-site and off-site storage of back-up copies of magnetic media was being maintained. We inspected the off-site location and determined that ORI's back-up copies of data files were locked in a fireproof safe within a secure room equipped with water sprinklers.

AUDIT RESULTS

1. ENVIRONMENTAL PROTECTION AND PHYSICAL SECURITY

We found that controls for environmental protection needed to be strengthened to provide a more suitable environment for the operation of computer equipment within the file server room. Physical security and environmental protection controls were determined to be adequate for the office and the off-site storage area. We found that there was an automatic sprinkler system in place for the office and the file server room. In addition, magnetic media was stored on site in a fireproof safe. The file server room also had an uninterruptible power supply (UPS), fan, and thermometers.

The building's general air conditioning system, while appropriate for the general office area during the summer, was inadequate to provide sufficient cool air for the file server room throughout the year. We noted from interviews and by observation that the temperature levels in the file server room were usually high, requiring the staff to leave the door open to obtain improved ventilation. We observed that temperature levels in the file server room were found to be excessively warm (76 degrees), and that temperatures would rise to a range of 85 to 88 degrees in the summer months, according to ORI staff members. To help alleviate this condition, agency staff leave the door to the file server room open regardless of whether someone is in the room. While this may help reduce the temperature levels, it decreases physical security over the file server room. Because the door, which has a lock, is left open during business and non-business hours, adequate physical security is not being provided to restrict unauthorized access to the file servers and magnetic media stored on-site. The physical security risks to the room include computer equipment and the on-site storage container of magnetic media. Visitors to the agency are required to sign-in, which does provide a degree of compensating control.

Generally accepted control practices and industry standards for IT operations indicate the need to prevent and detect overheating of facilities housing IT resources, such as microprocessors and file servers. In addition, these same generally accepted control practices support the need for each entity to have internal control policies and procedures for environmental protection controls, which ORI has not developed.

Recommendation:

We recommend that the ORI contact their building management to enquire as to whether there are ways that air circulation can be increased in the file server room to an acceptable level. If adequate air circulation, or dedicated air conditioning, for the file server room cannot be provided, we suggest that ORI consider requesting that air passageways near the ceiling level be installed for increased air flow. In addition, we recommend that ORI relocate the safe containing backup tapes to another office location until the air circulation problem has been resolved so that the file server room could be locked.

Auditee's Response

ORI agrees with the State Auditor that environmental controls need to be strengthened in the file server room. The State Auditor has correctly pointed out that the buildings general air conditioning system is inadequate to handle the demands of the file server room. The State Auditor has correctly identified the current trade off between security (server room door that should be locked for physical security purposes) and cooling (reducing the thermal buildup in the server room by keeping the door open for cooling the server room).

On several occasions, the office manager has requested that the building superintendent remedy the overheating problem in the file server room, to no avail. While some improvement has occurred, it is likely that only limited marginal improvements could be made with the landlord, mostly due to their unwillingness to accept responsibility for this issue.

ORI has been researching other possibilities, including the purchase a secure rack mount for the server from APS. APS (the makers of a line of Uninterruptible Power Supplies) has recently come to market with an secure enclosed rack that provides air circulation intake from the floor and exhaust into the ceiling plenum air return. ORI will identify the specifications for this application and seek internal funding to remedy this issue. Subject to funding, ORI will pursue this remedy.

ORI has moved the backup tapes safe out of the server room based on the recommendation of the State Auditor.

Auditor's Reply

We will review future progress at the next scheduled audit.

2. POLICIES AND PROCEDURES

Our audit revealed that although the Office for Refugees and Immigrants did maintain some IT-related policies and procedures, they were not sufficiently complete to address all IT functions.

Although there were policies and procedures for physical and logical access security, documented policies and procedures needed to be enhanced or developed to appropriately address environmental protection and inventory control of IT resources. There were no policies or procedures for control of hardware or software inventory, on-site or off-site storage of backup copies of magnetic media, or for business continuity and contingency planning.

Such documented policies and procedures would provide reasonable assurance that control and business objectives would be achieved. Formal documentation of IT-related policies and procedures provides a good basis for ensuring that desired actions are taken and that undesired events are prevented or detected and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff, serve as a good basis for evaluation, and increase communication among personnel to improve operating efficiency and effectiveness. Clearly, well-trained personnel develop a better understanding of their duties and improve their levels of competence when documented procedures are followed. The absence of formal standards and policies leads employees to rely on their individual interpretations of what is required to be performed to properly control IT-related systems. In such circumstances, management may not be adequately assured that desired actions will be taken.

Failure to provide documentation of policies and procedures, to provide a statement of internal controls, and to require audit and management trails seriously undermines the capability of auditing the system. Chapter 647 of the Acts and Resolves of 1989 requires that all state agencies have documented and approved internal control procedures. In addition, having documented and approved internal control procedures is also a generally accepted control practice.

Recommendation:

We recommend that the ORI add to and strengthen current IT-related policies and procedures in place for physical and system access security and include environmental protection, hardware and software inventory controls, and on-site and off-site storage of backup media, as well as business continuity and contingency planning, in order to provide sufficient documented guidance to IT operations. The development of documented policies and procedures should be focused on providing a control structure for managing IT processes and activities throughout

the office. We further recommend that ORI administrators develop and document procedures to ensure adequate monitoring and evaluation of documented internal control systems.

Auditee's Response

ORI agrees that additional documentation for IT policies that are undocumented should be written down. ORI will proceed to create the needed documentation in the following areas pointed out by the State Auditor:

a) Environmental Protection
b) Inventory Control
c) Control of hardware and software inventory
d) on-site and off-site storage of tape backup of magnetic media
e) business continuity planning
f) contingency planning

ORI agrees that "The absence of formal standards and policies leads employees to rely on their individual interpretations of what is required to be performed to properly control IT-related systems. In such circumstances, management may not be adequately assured that desired actions will be taken." see Ch. 647 of the Acts and Resolves of 1989. ORI will proceed to document these IT policies.

Auditor's Reply

We will review the new documentation at the next scheduled audit.

3. BUSINESS CONTINUITY AND CONTINGENCY PLANNING

We determined that the Office did not have a formal, written or tested business continuity and contingency plan to provide for the timely restoration of essential business functions should automated systems available through its local area network (LAN) be rendered inoperable. Although ORI had a year 2000 readiness plan, it had not been updated or tested since December 1999, and would not serve as an adequate business continuity plan due to its limited scope. Because the plan was developed for the specific purpose of testing applications and systems on January 1, 2000 for any date-related problems, it is inadequate since it does not cover possible scenarios where processing capabilities would be lost or significantly degraded.

Although the ORI had an agreement with their parent agency, the Executive Office of Health and Human Services (EOHHS), to provide workstations from which access to the application system could be gained, the agreement needs to be documented to cover responsibilities and

procedures to be followed should the alternate operations area be required. Furthermore, although EOHHS facilities are used to store backup media for off-site storage purposes, a written agreement of the required backup storage procedures and responsibilities was not in place. Although it is understood that EOHHS would make every effort to assist ORI, documentation of the business continuity support, including backup storage procedures, would strengthen the framework of internal controls. The agreement would include requirements and responsibilities regarding the provision of an alternate operations or processing site.

The objective of a business continuity and contingency plan is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for computer operations support the need to have an ongoing business continuity and contingency planning process that assesses the relative criticality of information systems and develops appropriate recovery and contingency plans, as required. To that end, ORI should assess the extent to which the Office is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical requirements of its information systems.

The assessment of impact should identify the extent to which ORI's business objectives and functions are affected over various time frames of the loss of processing capabilities. The assessment of criticality and impact of loss of processing should assist the ORI in triaging its business continuity planning and recovery efforts.

Recommendation:

The ORI should immediately establish a formal, written business continuity and contingency plan that incorporates criticality and impact assessments, risk management, business continuity plan development, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should be developed to ensure that the relative importance of the Office's systems is evaluated on an annual basis, or upon major changes to the IT infrastructure, application systems, or user requirements. The ORI should also conduct a formal risk analysis of its IT-related components on an annual basis, or upon major changes to the relevant IT

infrastructure, or to business operations or priorities. The plan should also include an alternative processing site and off-site storage of magnetic media.

Auditee's Response

ORI agrees with the State Auditor that ORI has not revisited their Business Continuity Plan since the Y2K readiness plan of 1999 which has not been updated or tested since December of 1999. ORI will proceed to document its agreement with EOHHS for Business Continuity.

ORI agrees with the statement of the State Auditor that, "ORI should immediately establish a formal, written business continuity and contingency plan that incorporates criticality and impact assessments, risk management, business continuity plan development, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should also be developed to ensure that the relative importance of the Office's systems is evaluated on a annual basis, or upon major changes to the IT infrastructure, application systems, or user requirements.

ORI will proceed to document the business continuity and contingency plans in writing.

Auditor's Reply

We will review the updated business continuity and contingency plans at our next scheduled audit.

GLOSSARY

GAGAS	Generally Accepted Government Auditing Standards.
LAN	(Local Area Network) A communications network that serves users within a confined geographical area. It is made up of one or more file servers, a network operating system, a communications link, and workstations.
Operating system	The operating system is a set of programs required for the computer to operate and manage programs and devices, such as printers, terminals and other peripherals. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk.
T1	A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires. T1 lines are used for heavy telephone traffic, or for computer networks linked directly to the Internet. T1 lines are normally used by companies with heavy network traffic.
Workstations	The workstations are the personal computers that are connected to the LAN and perform stand-alone processing and access the network servers as required.
WAN	(Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.