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. 2007-0432-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE REVIEW OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DEPARTMENT OF FISH AND GAME

January 1, 2005 to January 12, 2007

OFFICIAL AUDIT REPORT

MAY 25, 2007

TABLE OF CONTENTS

INTRODUCTION

The Department of Fish and Game (DFG or Department) was created in 1974 and placed within the purview of the Executive Office of Environmental Affairs (EOEA) under Chapter 21, Section 7 of the Massachusetts General Laws. Until January 2004, DFG was formally known as the Department of Fisheries, Wildlife and Environmental Law Enforcement. In 2004, the Division of Law Enforcement was placed within EOEA and renamed the Office of Law Enforcement (OLE). The DFG is charged with stewardship responsibility over the Commonwealth's marine and freshwater fisheries, wildlife species, plants, and natural communities. The Department's mission is to conserve and restore the state's rivers, streams, lakes, ponds, wild lands, and coastal waters through programs of research, restoration, and land protection. In addition, the Department issues licenses and registrations for hunting, trapping, and inland and marine fishing. The Department promotes recreational uses of the state's lands and waters consistent with the agency's mission.

The DFG is comprised of a Commissioner and approximately 300 employees and contract staff, including a Chief Financial Officer, General Counsel, and Chief information Officer. The Department consists of four main divisions: the Division of Fisheries and Wildlife (DFW); the Division of Marine Fisheries (DMF); the Riverways Program; and the Office of Fishing and Boating Access. The Department's information technology staff consists of an Acting Chief Information Officer, who currently oversees one full-time and one part-time employee. The DFG also enlists the services of two contracted information technology vendors that supply support staff for the SPORT application systems.

MassOutdoors is the on-line title given to the licensing and registration system provided through the Internet, but is formally known as the Statewide Point-of-Sale Outdoor Recreation Transaction (SPORT) system. This system was "designed as a web-based application system to provide one-stop-shopping for new and renewal recreational licenses, non-commercial lobster permits, and boat, ATV, and snowmobile registrations." New boat registrations are not fully addressed through the web-based application, because they require presentation of a certificate of title.

The SPORT application operates through three production file servers and two development servers. The development servers are intended to mirror the production servers and serve in an emergency as backup platforms. The database servers for production and development are located at the Causeway Street data center. The application server (internet) for production is located at One Ashburton Place, while the development server is located at the Causeway Street data center. The application server (point-of-sale) is located at the Causeway Street data center.

The database server supports an Oracle database and related Oracle components and provides the backend database capability for the SPORT application. The application servers provide front-end functionality that is largely written in Java. The Internet application server, because it has to communicate directly with the Internet, is located behind ITD's firewall and hence is situated in ITD's data center at One Ashburton Place. The point-of-sale application server is located at Causeway Street in close proximity to the principal point-of-sale location. The SPORT (MassOutdoors) system is supported by a "help desk" available through e-mail or voice mail 24/7.

The Office of the State Auditor's review focused on a review of selected general controls, including virus protection, and certain aspects of the SPORT application system.

SCOPE, OBJECTIVES, AND METHODOLOGY

***Scope*:**

Our review, which was conducted from November 28, 2006 to January 12, 2007, covered the period of January 1, 2005 to January 12, 2007. The purpose of our review was to determine whether corrective action had been taken to address IT-related control areas that had been brought to management's attention as a result of audit work covering the period of November 11, 2001 through February 28, 2005. The scope of our current review included a review of general controls regarding the organization and management of the Department of Fish and Game's (DFG or Department) IT environment, physical security and environmental protection over IT-resources in the data center and the Boston and Westborough administrative offices, system access security to the automated systems, inventory control of computer equipment, virus protection, business continuity planning, and on-site and off-site storage of backup copies of mission-critical and essential magnetic media. We also reviewed DFG's user satisfaction and help desk functions for the Sport application.

***Objectives*:**

With respect to IT-related controls, we sought to determine whether adequate IT organization and management controls were in place to properly support the Department's IT processing environment. We reviewed the documentation of IT-related internal controls, and sought to determine whether DFG had an agency-specific internal control plan and whether documented IT internal controls were sufficiently comprehensive and detailed to support agency business functions, including IT-related activities.

We sought to determine whether adequate controls regarding physical security and environmental protection were in place to safeguard computer operations and IT-related assets. A further objective was to determine whether adequate controls were in place to prevent and detect unauthorized access to DFG's primary application, software available through the Department's local area network and workstations, and its data files. With respect to hardware inventory, our objective was to determine whether IT-related assets were being recorded on the Department's inventory records.

We sought to determine whether appropriate controls were in place to prevent and detect viruses and unauthorized intrusions, assess the level of risk of viruses, report on the occurrence of a potential virus, and to implement corrective measures. Our examination focused on the degree to which corrective action had been taken to address virus protection controls as noted in our prior IT Audit Report No. 2004-0279-4T, issued on December 22, 2005. We also sought to review DFG's satisfaction and help desk functions associated with their primary application system.

We sought to determine whether DFG's business continuity plan would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should a disaster render computer systems inoperable or inaccessible. In conjunction with reviewing business continuity planning, we sought to determine whether proper backup procedures were being performed and whether copies of backup magnetic media were being stored in secure on-site and off-site locations.

***Methodology*:**

To determine our scope and objectives, we first obtained an understanding of DFG's mission, organizational structure, and primary business functions. We conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, reviewing our prior audit conclusions and recommendations, performing a preliminary review of IT-related internal controls, and interviewing senior management to discuss the IT control environment. We performed a preliminary walkthrough of the data center and office areas housing workstations.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the IT organizational structure and reporting lines of the DFG's IT staff. We obtained and reviewed relevant IT-related policies and procedures and IT strategic plans with respect to IT governance and direction.

To evaluate physical security, we determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to areas housing microcomputer workstations and IT resources, and whether authorized personnel were specifically instructed in physical security policies and procedures. We assessed DFG's physical security controls and determined the extent to which physical access was restricted for areas housing computer equipment by conducting a walkthrough of the office area and data center. We examined for the existence of controls, such as keypad access, motion detectors, and intrusion alarms. We evaluated the location of the data center with respect to physical security controls.

To determine whether adequate environmental controls were in place to properly safeguard automated systems in the data center and areas housing workstations from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply, and emergency lighting. To determine whether proper temperature and humidity controls were in place, we reviewed the presence of appropriate air conditioning units in the data center. In addition, we reviewed environmental protection related to general housekeeping procedures in the data center and selected areas housing workstations.

To determine whether adequate controls were in place to prevent and detect unauthorized access to DFG's primary application and its data files, we obtained and reviewed DFG's policies and procedures related to system access security, interviewed IT staff responsible for authorizing, maintaining, and altering user privileges, and evaluated access security issues brought forward in our prior audit review. We also obtained, reviewed, and confirmed a list of DFG staff and consultants authorized to access and make changes to the SPORT application by comparing the personnel noted on the system list to departmental payroll and vendor records.

To determine whether computer equipment was properly identified and recorded in DFG's inventory records, we obtained and reviewed DFG's policies and procedures related to fixed-asset inventory controls, obtained and reviewed a copy of DFG's computer equipment inventory, reviewed the computer equipment inventory for necessary fields of information, and interviewed IT staff regarding inventory controls. With respect to the Department's adherence to applicable laws and regulations regarding fixed assets of the Commonwealth, we interviewed management to evaluate compliance with Chapter 647 of the Acts of 1989 and fixed-asset management regulations from the Office of the State Comptroller's "Internal Control Guide for Departments." Chapter 647 requires that state entities report lost or stolen equipment to the Office of the State Auditor. We also reviewed policies pertaining to the accounting of assets, including Office of the State Comptroller's Memos 310 and 313A. In addition, we also interviewed management to determine whether the DFG complied with 802 Code of Massachusetts Regulations (CMR) 3.00 entitled "Disposition of Surplus State Property."

To determine whether corrective action had been taken with respect to areas we found deficient in our original evaluation of virus protection at DFG, we reviewed the virus protection software and updates, associated policy and procedure documentation, and a schematic of the network and computer workstations. These documents enabled quick access to virus-affected machines for immediate shut down. We also interviewed the Acting CIO pertaining to virus and unauthorized intrusion detection and protection for DFG's automated systems.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the Department's computer systems be damaged or destroyed. We interviewed management in reference to written manual procedures used by the Department to maintain on-going work functions if computer resources were unavailable for a long duration of time. In addition, we interviewed the Acting CIO and senior management as to whether the written business continuity plan had been tested and was in effect, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Furthermore, to evaluate the adequacy of controls to protect computer–based data files and software, we interviewed DFG business staff responsible for creating backup copies of computer-related media. Further, we inspected the storage locations for the Department’s on-site and off-site backup media.

Our review included interviews with relevant staff and management, a review of prior audit work-papers and relevant DFG documentation, and on-site observations. We did not examine or test application controls over the MassOutdoors application, which is the Internet name for the SPORT application, at this time because we had not detected control deficiencies during the prior review period nor had management informed us of control concerns during this review. We did, however, review IT-related policies and procedures for the areas included in our scope, and performed limited testing pertaining to system access security, physical security and environmental protection controls. As a result of our review, certain observations were made regarding the existing control environment that are presented in this report to assist the Department’s efforts in ensuring that adequate IT-related controls are in place and in effect.

SUMMARY

Our review indicated that although improvements in control practices had been made since our prior review, IT general controls in certain areas needed to be strengthened, documented, and monitored. With regard to IT organization and management, we found that formal internal control policies for IT-related activities needed to be enhanced for physical security, environmental protection, system access security, inventory control for computer equipment, and business continuity planning. To strengthen the overall IT environment and ensure that IT control objectives will be met, the Department of Fish and Game (DFG or Department) should develop and implement a comprehensive IT governance and control framework. Although we found IT strategic plans in place, management should develop IT tactical plans to identify IT initiatives, tasks and activities with targeted milestones.

We determined from our review that policies and procedures were not adequately documented and that controls needed to be strengthened for the physical security and environmental protection of the Department's file servers. Concerning system access security, we found policies and procedures were adequate and in place regarding logon ID and password administration. With respect to virus and intrusion protection of the local area network, we found the Department had installed centralized anti-virus controls, created server logs viewable for risk analysis, and the IT department performs periodic network risk and security analysis. In addition, we found that the level of virus protection and associated policy and procedure documentation had addressed the deficiencies noted in our October 27, 2004 virus protection survey.

We determined that DFG did not have a formal policy and procedure regarding inventory control over computer equipment. We also determined that the inventory system of record was not sufficiently complete and did not take full advantage of available data fields. To ensure proper internal controls, including appropriate segregation of duties, the staff who performs the periodic reconciliation should not be responsible for maintaining the Department's inventory system of record.

Although the Department had a Continuity of Operations Plan (COOP) in place for its divisions, we determined that the plans were not sufficiently comprehensive to ensure that in the event of a disaster, mission-critical systems and essential IT operations could be regained within an acceptable period of time. Without a comprehensive formal and tested recovery and contingency plan, DFG's ability to regain critical processing capabilities would be impaired.

Based on our interviews with IT management, we determined that the Department has appropriate controls in place and adequate coverage of its help desk. Our review indicated that DFG management stated that the system is stable and functioning as intended, and nothing came to our attention during our review to indicate control concerns regarding system availability and security.

REVIEW RESULTS

1. IT Organization and Management

Our review of IT organization and management at the Department of Fish and Game indicated that although certain control procedures, strategic planning mechanisms, and a defined organizational structure existed, IT organization and management controls needed to be strengthened. We found that DFG's IT strategic plans were adequate to identify and set management direction. We also found that there were defined reporting lines for the limited number of IT staff at DFG. However, we found that formal internal control policies for IT-related activities needed to be enhanced for physical security, environmental protection, inventory control for computer equipment, and the generation and on-site and off-site storage of backup copies of magnetic media.

The absence of a clearly-defined and workable process to develop, promulgate, and ensure adequate understanding and compliance with IT policies, standards and procedures significantly inhibited the issuance and implementation of appropriate IT-related policies and standard procedures. For example, with respect to business continuity and disaster recovery, we found that a sufficiently comprehensive disaster recovery plan for IT operations had not been developed and consequently tested. Although DFG had certain control procedures in place to assure operational efficiency and the ability to meet its primary business objectives, a set of formal policies and procedures had not been adequately documented in an internal control plan for IT functions. As a result, if a disaster were to occur, the restoration of automated systems that are supported by the IT department could not be attained within an acceptable period of time, thereby jeopardizing essential DFG operations. We recommend that the Department enhance its documented policies and procedures with respect to all IT functions and activities. The Department would benefit from developing and implementing a comprehensive IT governance and control framework to ensure that control objectives will be met.

We also found that DFG did not have a formalized process for developing and maintaining IT strategic and tactical plans. Without comprehensive strategic planning, the analysis and development processes may vary substantially among projects, potentially resulting in information systems that may be inefficient, incompatible, or have cost overruns on development or system maintenance. We recommend that the Executive Office of Energy and Environmental Affairs collaborate with the Department to develop strategic plans to address all IT initiatives, projects, and functions, including data center operation, inventory control, and IT configuration management. Based on the IT strategic plans, management should develop IT tactical plans to identify IT department initiatives, tasks and activities with targeted milestones.

Auditee's Response:

> *We do agree that more IT policy documentation and monitoring is a good thing…(see full text of Auditee's Response in Appendix A – Auditee's Response).*

Auditor's Reply:

We believe that DFG should work with EOEA to formally document IT policies and procedures to ensure operational efficiency for their IT environment.

2. Physical Security

Based on our review of the policies and procedures received from DFG's IT staff, observations, and interviews with management and staff, we determined the Department's policies and procedures were not adequately documented, or in place and in effect, for the physical security over the file servers located in the basement of the facility. Our review was limited to the fourth floor administrative offices, one regional site, and DFG's data center in Boston, Massachusetts.

Although we found adequate physical security controls in place in the administrative offices housing DFG workstations and the one regional site we reviewed, we found that physical access security controls in the data center housing the Department's SPORT servers needed to be strengthened. Our review disclosed that the DFG has four file servers located within the EOEA data center. The Executive Office of Energy and Environmental Affairs is the oversight agency responsible for the physical access security controls over the data center located in the basement at 251 Causeway Street. The data center is accessible by a swipe card, which records access data for those entering the data center. The Department maintains a formal list of DFG-authorized IT staff, approved by the CIO, who has access to the data center. However, no logs are maintained of visitors entering the facility with a cardholder. Although the door appears to be kept locked when not in use, the door to the data center opens into a corridor in the basement of the building, accessible by the public. According to the Department, the data center has neither a motion detector nor an intrusion alarm to note unauthorized access. The data center has two street-level windows that are neither alarmed nor barred. We found that there are no surveillance cameras to record activity located at the entry to the data center or at the windows. The server room is under the control of the EOEA's IT department.

Generally accepted computer industry practices indicate that appropriate physical security controls need to be in place to ensure that the information technology assets are operating in a safe and secure processing environment. Computer assets should be protected and properly safeguarded against loss or damage. The Department should adopt appropriate physical security policies and procedures requiring that computer assets be protected from unauthorized access, use, damage, or theft. We recommend that

DFG seek solutions with EOEA to establish control mechanisms to address the potential weaknesses regarding street level egress noted above in the data center.

Auditee's Response:

> *The department has noted the additional recommendations for further enhancements of the data center physical security…(see full text of Auditee's Response in Appendix A – Auditee's Response).*

Auditor's Reply:

We continue to urge the Department to work in conjunction with EOEA to seek a more appropriate location for the placement of the data center in order to reduce the risk of damage to equipment and the loss of processing capabilities.

3. Environmental Protection

Although we found certain environmental protection controls in place at the administrative offices and the data center, environmental protection controls needed to be enhanced in the area housing DFG's file servers. Our review revealed that the Department maintained an emergency evacuation plan for the entire building, fire extinguishers, and air conditioning for areas housing the servers. Environmental protection controls were in place and were adequate for the administrative office environment. We also found an uninterruptible power supply device in place at the data center to permit a controlled shutdown and to prevent a sudden loss of data. However, we found that there were no documented policies at DFG regarding environmental protection controls. We also observed that general housekeeping at the data center was poor, and there were other appliances and devices plugged into extension units throughout the data center as well as wires hung across the ceiling held up with paper and butterfly clips.

Although the data center did have a sprinkler system, smoke and fire detection devices, and emergency lighting, there were no water detection devices. The location of the Department's servers was directly below one of the sprinklers and therefore the server would be damaged either upon activation or from water retention in the basement. Since the servers support the SPORT application and are critical to the business objectives of DFG, management should consider moving the servers to a more secure and environmentally protected area.

Generally accepted computer industry practices indicate that appropriate environmental protection controls need to be in place to ensure that the information technology assets are operating in a safe and secure processing environment. Computer assets should be protected and properly safeguarded against loss or damage due to heat, humidity, water, or fire. Appropriate environmental protection controls also serve to protect employees or other persons from undue harm.

The weaknesses in controls over environmental protection were discussed with DFG management during our review. However, to improve physical security and environmental protection over the data center, DFG management should coordinate their efforts with EOEA, which controls the data center. We recommend that DFG collaborate with EOEA to establish policies and controls to address the weaknesses noted in the data center.

Auditee's Response:

> *The department has noted the additional recommendations for further enhancements of the data center physical security, environmental protection…(see full text of Auditee's Response in Appendix A – Auditee's Response).*

Auditor's Reply:

We continue to urge the Department to work in conjunction with EOEA to seek a more appropriate location for the placement of the data center in order to reduce the risk of damage to equipment and the loss of processing capabilities.

4. System Access Security

We found that the policies and procedures in place regarding system access security for the SPORT application, including logon ID and password administration, were adequate. The Department has direct control over system access to the SPORT application. Our review of user accounts for eight individuals allowed to authorize and modify access privileges for DFG system users indicated that these individuals were current employees and possessed appropriate levels of user privileges. Since access to the WAN, HR/CMS and MMARS are coordinated with and controlled by other agencies, we did not review access privileges to the wide area network or these application systems. During the course of our audit, nothing came to our attention to indicate that there were weaknesses in system access security control procedures at DFG.

Auditee's Response:

> *We were pleased to note the positive comments contained in two of your review areas regarding system access security and virus protection (see full text of Auditee's Response in Appendix A – Auditee's Response).*

Auditor's Reply:

No comment necessary.

5. IT-related Inventory

Our review of the DFG's policies and procedures regarding inventory control over computer equipment disclosed that the DFG did not have formalized policies and procedures for inventory control at the time of our review. The Department was able to provide an inventory system of record for computer equipment with data fields that included item description, date acquired, purchase amount, IP address, location, and asset tag number. However, DFG did not have complete information within the system of record for the available data fields for date acquired and cost to support IT configuration management. A review of the inventory data revealed that a significant portion of the data was incomplete for data acquired and cost. For example, there were no cost figures recorded for 216 out of 418 IT resources listed. In addition, the inventory did not list tag numbers for over 200 IT resources.

We acknowledge that the recording of IP addresses for microcomputers and servers strengthens the inventory data and encourage the Department to obtain a full listing. We found that 69 of the 314 microcomputer systems listed contained Boston IP addresses. We also found that the system of record did not contain the names of all parties to whom notebook computers may have been assigned. While it is possible that notebooks not having a staff name listed had not been assigned, it would strengthen the inventory record to indicate “not assigned” where appropriate. We also note that there were no sign out/in procedures for controlling the provisioning of notebooks. As a result, a register listing the assignment of notebook computers was not being maintained.

We found that the inventory system was not always maintained on a perpetual basis. Although it is our understanding that the inventory had been reconciled prior to our audit period, there was no evidence that the inventory had been reconciled during the current audit period. While inventory systems provide a basis for properly recording property and equipment, the IT inventory record can also support IT configuration management and safeguarding of IT resources. By failing to record the proper information for computer equipment on the DFG’s inventory system of record, the Department was not in full compliance with the Commonwealth of Massachusetts Comptroller’s Office’s fixed assets requirements and Comptroller’s Memo 313A.

We recommend that DFG maintain the IT inventory on a perpetual basis and that physical inventory and reconciliation of the inventory system of record be performed either on a cyclical basis or at least annually. The perpetual inventory record of IT resources, including computer equipment, should be periodically verified through reconciliation to computer equipment acquisition, records of lost or stolen equipment, and disposal records. We also recommend that DFG review the inventory system of record and update information for missing, inaccurate or incomplete fields of information. To enhance the inventory, we recommend that IT resource status be included to support IT configuration management. On addition, to further strengthen inventory control and IT security, DFG should ensure that all staff assigned a notebook computer complete sign-out/in forms and that the status of the computers be periodically monitored for need, location and assignment.

Auditee's Response:

> *The department has noted the additional recommendations for further enhancements of the…IT related inventory…(see full text of Auditee's Response in Appendix A – Auditee's Response).*

Auditor's Reply:

The Department should enhance their inventory control system for computer equipment and complete a physical inventory and reconciliation process. Once a system is in place, the Department should continue to monitor the system of record for computer equipment on a perpetual basis.

6. Virus Protection

Regarding virus and intrusion protection on the Department's local area network, we found that DFG has installed centralized anti-virus controls that include server-based automatic virus signature updating and scanning. The Department has also created server logs viewable for risk analysis, and the IT department performs periodic risk and security analysis on the network by port scanning and inspection of server logs. According to the Department, the Causeway Street office has not been the source of any network virus infection over the last five years. Also, to address the results and findings of our prior IT Audit Report No. 2004-0279-4T, issued on December 22, 2005, we reviewed documented policies, procedures, and controls to address virus attacks and unwanted intrusions. We note that there has been an effort to improve the policies, procedures, and controls, which are now in place and in effect. We recommend that further effort regarding the level of documentation for formal policy development in the area of virus protection may be warranted.

Auditee's Response:

> *We were pleased to note the positive comments contained in two of your review areas regarding system access security and virus protection (see full text of Auditee's Response in Appendix A – Auditee's Response).*

Auditor's Reply:

The Department should continue to modify virus protection updates as risks and vulnerabilities to their IT environment change.

7. Business Continuity and Disaster Recovery Plan

Our review revealed that although the Department had a Continuity of Operations Plan (COOP) in place for its divisions, the plans presented were not sufficiently comprehensive to provide reasonable assurance that mission-critical systems and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable. The COOPs are more of a “to do” list to be followed after an occurrence, and they lack the necessary information to actually carry out the plans. For example, some of the completed sections contain instructions noting what should be done, but do not identify who is responsible for carrying out the tasks. In addition, the plans have not been tested.

At the time of our review, no manual work-around procedures for the various computer-related business functions were included as part of the business continuity planning. Interviews with management revealed that many of the procedures are written to allow for manual processing of business functions, as many of the licenses and permits can be issued offline. Given the absence of an adequate business continuity plan, a significant disaster impacting the DFG’s SPORT application could seriously affect the daily operations of the system.

Auditee’s Response:

> *We do agree that… additional business continuity planning for both the short term and long term needs to be strengthened.*
>
> *We do however disagree somewhat with the conclusions reached regarding the generation and storage of backup media. All of the department servers over which we have control (i.e. SPORT servers and our GIS/anti-virus/patching server) are backed up regularly with tapes stored off-site at a secure location. Additionally, either EOEA or ITD provide backup services for the other servers with which we are also involved (see full text of Auditee’s Response in Appendix A – Auditee’s Response).*

Auditor’s Reply:

We commend the Department for recognizing the need for a comprehensive business continuity strategy and plan. Once the plan is fully developed and implemented, the plan should be periodically tested to ensure its viability.

8. SPORT Application System

Help Desk

During the prior audit period, the SPORT application was a newly installed system, necessitating a full time help desk. While the help desk provides a valuable service, the Acting CIO believes that there is no longer a need for a full time help desk. The part time employee assigned to help desk tasks primarily provides informational assistance. The application runs smoothly with infrequent errors and interruption in service. There is a formal procedure to document, report, investigate, and correct any program problems. According to IT management, the SPORT application system runs on a 24/7 basis with virtually no unscheduled down time.

SPORT Performance

Based on interviews and our review of documentation supplied by DFG management, the on-line licensing and registration system, originally known as the Statewide Point-of-Sale Outdoor Recreation Transaction (SPORT) system, adequately supports the mission of DFG by providing a comprehensive approach for registering and licensing recreational vehicles and permits for non-commercial lobstering. We also interviewed DFG management for a current assessment of the Massachusetts Department of Fish and Game's Licensing and Registration System, otherwise known as SPORT. Revenue growth over the past four fiscal years (2003 to 2006) for licenses and registrations increased from $5,617,531 to $7,262,639. It was further noted that during this 4 year period, the Internet portion of this revenue increased from $999,160 to $1,994,926.

Auditor’s Reply:

No comment necessary.

Auditee's Response

Commonwealth of Massachusetts
Department of Fish and Game
251 Causeway Street, Suite 400
Boston, Massachusetts 02114
(617) 626-1500
fax (617) 626-1505

Deval L. Patrick
Governor
Timothy P. Murray
Lieutenant Governor

Ian A. Bowles
Secretary
Thomas W. French
Acting Commissioner

Mr. Frank Cintolo, Audit Director
Office of the State Auditor
One Ashburton Place
Room 1819
Boston, MA. 02108

Dear Mr. Cintolo:

I want to thank you for the opportunity to meet, review and comment on the draft report on the "Review of Information Technology-Related Controls at the Department of Fish and Game. During this review period, department staff attempted to provide accurate and complete information to the field auditors. In this response, we will provide additional points of clarification where we feel essential formation was not included in this draft.

For the most part, we have no substantial disagreements with the Review's overall conclusions and recommendations. We do agree that more IT policy documentation and monitoring is a good thing, as is the recommendation that additional business continuity planning for both the short term and long term needs to be strengthened.

We do however disagree somewhat with the conclusions reached regarding the generation and storage of backup media. All of the department servers over which we have control (i.e. SPORT servers and our GIS/anti-virus/patching server) are backed up regularly with tapes stored off-site at a secure location. Additionally, either EOEA or ITD provide backup services for the other servers with which we are also involved.

We were pleased to note the positive comments contained in two of your review areas regarding system access security and virus protection. The department has noted the additional recommendations for further enhancements of the data center physical security and environmental protection, IT related inventory and business continuity planning and will endeavor to implement the changes.

We also look forward to taking up Deputy Auditor John Beveridge on his offer to provide additional information and training in setting up a comprehensive IT framework for the department.

Staff will be working over the upcoming months to carry out the recommendations contained in this review. We have a small staff, but will proceed as rapidly as possible. Finally, we will endeavor to cooperate with any efforts and solutions that EOEA may propose for remedying their data center problems, as it will also be beneficial to this department and its users.

In closing, if you need any additional information or need any meeting time, please note that I will make myself and staff available at your convenience.

Sincerely,

Thomas W. French
Acting Commissioner

Cc: Philip Griffiths, EOEEA
John Beveridge, OSA
Brian M. Kelter, DFG
Stephen D. McRae, DFG
File: OSA/IT Review