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. 2009-0432-7T

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

January 12, 2007 through May 15, 2009

OFFICIAL AUDIT REPORT

DECEMBER 18, 2009

TABLE OF CONTENTS

INTRODUCTION

The Department of Fisheries, Wildlife and Environmental Law Enforcement 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. In January 2004, the Department's name was changed to the Department of Fish and Game (DFG) and its Division of Law Enforcement was renamed as a separate entity under EOEA as the Office of Law Enforcement. In 2007, the Executive Office of Environmental Affairs was renamed the Executive Office of Energy and Environmental Affairs.

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. The Department also issues licenses and registrations for hunting, trapping, and inland and marine fishing. The Department promotes recreational use of the state's lands and waters consistent with the agency's mission. DFG received a state appropriation of $19,128,636 for fiscal year 2009.

At the time of our audit, DFG was 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. DFG also enlists the services of two contracted information technology vendors that provide support staff for the Department's licensing and registration system, referred to as MassOutdoors.

The MassOutdoors system, which was formally known as the Statewide Point-of-Sale Outdoor Recreation Transaction (SPORT) application system, was designed as a web-based 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 MassOutdoors application operates through three production file servers and two development servers. The development servers are intended to mirror the production servers and would serve in an emergency as backup platforms to support recovery efforts. The database servers for production and development are located at the Causeway Street file server room. The application server (for access via

the Internet) for production is located at One Ashburton Place, while the development servers are located at the Causeway Street file server room.

The database server supports an Oracle database and related Oracle components and provides the backend database capability for the MassOutdoors application. The application servers provide front-end functionality that is largely written in Java. The Internet application server is firewall protected and is located at the Commonwealth's Information Technology Division's (ITD) data center. The point-of-sale application server is located at Causeway Street in close proximity to the principal point-of-sale location.

The Office of the State Auditor's examination focused on a review and evaluation of certain controls pertaining to the MassOutdoors application system and DFG'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) general controls examination of IT-related activities at the Department of Fish and Game (DFG) for the period of January 12, 2007 through May 15, 2009. The scope of the audit consisted of an evaluation of the status of audit results from our prior audit report, No. 2007-0432-4T, issued May 25, 2007, regarding IT organization and management, physical security, environmental protection, system access security, inventory of computer equipment, virus protection, disaster recovery strategy and business continuity planning, and the MassOutdoors application. In addition, we examined internal controls over selected IT functions pertaining to virus protection. The audit was conducted from January 21, 2009 through May 15, 2009.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results and to review selected IT-related controls. We sought to determine whether IT-related controls were in place and in effect to support DFG's IT processing environment. In this regard, we sought to determine whether DFG'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.

Our audit objective regarding IT organization and management activities was to determine whether the organizational structure was appropriate and whether the auditee was maintaining key documentation, such as a mission statement, IT job descriptions, and a network topology document. We also sought to determine whether the auditee was maintaining an up-to-date internal control plan that reflected information technology operations.

Our audit objective regarding physical security controls was to determine whether IT-related policies and procedures were in place and in effect to ensure that only authorized users had physical access to IT resources in order to prevent unauthorized use, damage, or loss. We also sought to update the status of corrective action taken regarding prior audit results related to physical security.

We determined whether sufficient environmental protection controls were in place to provide a controlled operating environment and to prevent and detect damage to computer equipment and data. We also sought to update the status of corrective action taken regarding prior audit results related to environmental protection.

Our objective regarding system access security for software applications was to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to DFG's application systems and data files.

Our audit objective regarding virus protection was to review policies and procedures to determine whether controls had been implemented to provide reasonable assurance that viruses or unwanted intrusions would be prevented and, if detected, that appropriate incident response procedures would be followed.

Our objective regarding inventory control over computer equipment was to determine whether controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded and accounted for. We also sought to update the status of corrective action taken regarding prior audit results related to inventory control of computer equipment.

Regarding disaster recovery and business continuity planning, we sought to determine whether IT operations could be regained within an acceptable period of time through a comprehensive disaster recovery and business continuity strategy should systems be rendered inoperable or inaccessible. We also sought to determine whether adequate controls were in place to provide reasonable assurance that backup copies of magnetic media were generated and stored on site and off site to assist recovery efforts.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding DFG's overall mission and IT environment. Regarding our review of IT policies and procedures, we interviewed senior management and staff, completed questionnaires, and obtained and reviewed existing IT-related policies and procedures. For selected IT functions, we assessed the extent to which existing documented policies and procedures addressed the IT functions. We also interviewed DFG staff regarding the extent to which IT policies and procedures were documented and formalized. We also reviewed the DFG internal control plan to determine whether it included or referenced IT control guidelines and practices and, if so, whether the IT controls were adequately documented and current.

To evaluate physical security, we interviewed management, conducted walk-throughs, and reviewed procedures to document and address security violations and/or incidents. The areas reviewed were administrative offices, the file server room, and the on-site storage location at DFG. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment. We examined the existence of controls, such as office door and window locks, remote cameras, and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees or authorized consultants of DFG.

To evaluate whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we conducted walk-throughs of areas housing IT equipment and examined the adequacy of documented IT policies and practices pertaining to environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

To obtain an understanding of access security controls, we reviewed DFG's access security policies and procedures designed to prevent unauthorized access to the applications systems and data files accessible through the Department's workstations. Our test of system access security controls included a review of access privileges for employees and consultants who were authorized to access DFG application systems. To determine whether system access security was being properly maintained through the management of user IDs and passwords, we compared the DFG network user list to a roster of all DFG employees and consultants. We examined access to the mission-critical MassOutdoors application and the Massachusetts Management Accounting and Reporting System (MMARS). We also reviewed password administration controls, such as activation and deactivation, password length and composition, and the frequency of password changes.

We reviewed virus protection policies and procedures, including incident response procedures, to determine whether they were sufficiently detailed and in effect. We also observed and evaluated DFG's virus scan procedures that were performed on the Department's network.

To determine whether adequate controls were in place and in effect to properly account for DFG's computer equipment, we reviewed relevant inventory control procedures, interviewed individuals responsible for inventory control, and obtained and tested the inventory record of computer equipment. We examined policies and procedures regarding IT inventory control to determine whether DFG was in compliance with the Office of the State Comptroller's regulations regarding IT asset control.

We reviewed the inventory listing to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of IT-related computer equipment. We determined that DFG's perpetual inventory listing of IT-related items, as of February 28, 2009, consisted, in part, of three file servers, seven printers, eight notebook computers, and 77 desktop workstations. We also performed data analysis on the inventory to identify any duplicate records, unusual data elements, or missing values. To determine whether DFG's computer equipment was recorded on the inventory listing, we selected 60 items, or 60% of the total population of 101 items recorded on the DFG IT inventory listing of February 28, 2009, and verified their location and determined whether the inventory record properly recorded the description, identification, tag number, and location for the computer

equipment selected in our sample. We verified the physical inventory by tracing selected items from the DFG inventory listing to the floor, including eight notebook computers. We also verified actual locations, assigned users, serial numbers, and other related information for the notebook computers recorded on the inventory list.

To determine whether DFG complied with Commonwealth of Massachusetts regulations for accounting for assets, we reviewed evidence supporting DFG's performance of an annual physical inventory of IT assets. Furthermore, to determine whether DFG had complied with Commonwealth regulations for disposal of surplus property, we reviewed records and supporting documentation for computer equipment disposed of during the audit period. Finally, to determine whether DFG's staff were aware of, and in compliance with, Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen assets, we reviewed documented inventory control policies and procedures, interviewed senior management to determine whether DFG had had any incidences of missing or stolen IT-related equipment during the audit period, and verified whether any incidents were reported to the Office of the State Auditor.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether DFG, in conjunction with its governing body, the Executive Office of Energy and Environmental Affairs, had any formal documented plans or strategy to resume computer operations should the network application systems be rendered inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We interviewed senior management to determine whether DFG had formally documented procedures for the development and maintenance of appropriate business continuity plans. We also determined the extent to which DFG had performed a risk analysis with regard to the loss of IT-enabled business operations under different disaster scenarios. We evaluated the extent to which DFG had recovery plans that could be activated to resume IT-supported operations should the network and servers be rendered inoperable or inaccessible. As part of our examination of business continuity planning, we assessed the adequacy, generation, and storage of backup copies of magnetic media, and physical security and environmental protection controls for on-site storage. In that regard, we interviewed IT staff responsible for creating and storing backup copies of computer-related media. We further sought to determine whether DFG's IT personnel were aware of, and trained in, all procedures required to restore systems via backup media that would be required under disaster or emergency circumstances.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for

Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association in July 2007 and the Office of the State Comptroller's regulations.

AUDIT CONCLUSION

Based on our audit at the Department of Fish and Game (DFG), we found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to physical security and environmental protection for computer equipment located in office areas, system access security, virus protection, and inventory control over computer equipment. We found, however, that physical security controls needed to be enhanced to protect computer equipment located in the server room, and that disaster recovery and business continuity planning needed to be strengthened to ensure that IT systems could be restored and business operations regained within an acceptable period of time.

Although we determined that certain IT policies and procedures were in place, the level of formal documentation needed to be enhanced for physical security, environmental protection, inventory control over computer equipment, and disaster recovery and business continuity planning. The absence of sufficiently documented controls increases the risk that desired control practices would not be adequately communicated, administered, or enforced.

Although we found adequate physical security controls in place in the administrative offices housing DFG workstations, physical access security controls in the file server room housing the Department's MassOutdoors servers needed to be strengthened. DFG's mission-critical MassOutdoors application system and data files are operated and stored at the Executive Office of Energy and Environmental Affairs' (EOEEA) file server room. Although the file server room was locked, "swipe" card access was required, and the Department maintained a list of individuals authorized to access the room, security could be improved as there were no intrusion alarms, the room had street-level windows, and a list of visitors to the facility was not maintained. We also found that there were no surveillance cameras to record activity at the file server room's entrance or windows.

Adequate environmental protection, such as sprinkler systems, hand-held extinguishers, and a dedicated air conditioner were found to be in place in the file server room to help prevent damage to, or loss of, IT-related resources. We observed that the file server room was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We also found an uninterruptible power supply device in place at the file server room to permit a controlled shutdown and to prevent a sudden loss of data. We observed, however, that wires hung across the ceiling were held up with paper clips and butterfly clips, and that documented policies and procedures did not adequately address environmental protection.

Although the file server room had 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, placing the servers at potential risk of damage from sprinkler activation or from water retention. Since the servers support the MassOutdoors application and are critical to DFG's business objectives, management should consider relocating the servers to a more secure and environmentally protected area. In addition, although the Department maintained an emergency evacuation plan for its offices, the evacuation and emergency procedures were not posted within the office areas.

We determined that system access security policies and procedures were sufficiently detailed and had been formalized as official policies and procedures after being submitted to senior management for review and approval. We found that system access controls provided reasonable assurance that only authorized users had access to DFG's software programs and data files residing on DFG's file servers and microcomputer workstations. We determined that system access privileges granted to individuals were appropriate for their job responsibilities and functions. We found that administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should DFG employees terminate employment or incur a change in job requirements. Our tests confirmed that all current system users were DFG employees or authorized consultants. Through observation and interviews, we determined that password composition and changes to passwords were adequately controlled for access through DFG's IT network.

We determined that virus protection policies and procedures were sufficiently detailed and had been formalized as official policies and procedures after being submitted to senior management for review and approval. We also observed DFG performing a virus scan and determined that DFG was effectively monitoring unwanted intrusion attempts on its mission-critical software application. We determined that DFG had appropriate incident response procedures to be followed should a virus be detected or IT resources become infected.

With respect to inventory control over computer equipment, we found that DFG was in compliance with fixed-asset policies and procedures promulgated by the Office of the State Comptroller (OSC) and had conducted an annual physical inventory and reconciliation. In addition, we found that DFG was maintaining an up-to-date perpetual inventory system of record that included all required asset information. Our inventory control test as of February 28, 2009 disclosed that computer equipment was locatable and had been properly recorded on the inventory listing with, for example, correct description, location, tag numbers, and serial numbers.

Although the Department's eight notebook computers were properly recorded on the inventory system of record, the Department lacked a formal policy to control the assignment and use of notebooks. We

determined that DFG had assigned notebook computers to employees without requiring signed acceptance of the responsibility for security and authorized use. The lack of a formal policy to control notebook computers could hinder DFG's ability to safeguard and properly account for available computer equipment.

We found that DFG had not complied with the Operational Services Division's (OSD) policies and procedures regarding surplus Commonwealth fixed assets by not having properly obtained surplus status for the computer equipment items that were classified as obsolete and had not disposed of these items during the audit period. Our review for compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that DFG staff responsible for inventory were aware of the reporting requirements and that DFG did not have any occurrences of missing or stolen computer equipment during the audit period.

Our audit disclosed that DFG did not have a formal, tested disaster recovery and business continuity plan to provide reasonable assurance that the MassOutdoors application system and essential information technology could be regained effectively and in a timely manner should a disaster render automated systems inoperable. Although DFG had an informal framework of disaster recovery strategy, dated December 2008, for the MassOutdoors application and a DFG Continuity of Operations Plan (COOP), dated January 2009, the disaster recovery strategy and COOP needed to be further developed and integrated to provide detailed plans to address recovery strategies. At the time of our audit, the Department had not finalized its designation of an alternative processing site, and user plans had not been established to document the procedures to be followed to support business continuity objectives in the event of a loss of IT operations. We found that adequate procedures were in place regarding the generation of daily backup copies that were physically stored on site and transferred on a weekly basis to a secure off-site location.

AUDIT RESULTS

1. Prior IT Audit Results Unresolved - Disaster Recovery and Business Continuity Planning

Our prior audit, No. 2007-0432-4T, revealed that the Department of Fish and Game (DFG) did not have a documented business continuity plan in which detailed disaster recovery strategies would be included. We found that DFG had taken steps to address business continuity planning by implementing off-site storage of backup media and had begun the process of identifying a viable alternate processing site. In addition, DFG had an informal disaster recovery strategy, dated December 2008, to regain operation of the MassOutdoors application and a DFG Continuity of Operations Plan (COOP), dated January 2009. However, we determined that further effort was needed to develop and subsequently test detailed recovery strategies that would address various disaster scenarios. A validated recovery plan would provide reasonable assurance that mission-critical and essential business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. Moreover, although DFG understood that a loss of IT capabilities would adversely impact operations, a formal assessment of the relative criticality of the automated systems and the extent of potential risk and exposure to business operations had not been documented. DFG lacked a comprehensive business continuity strategy that would help ensure timely restoration of DFG systems.

At the time of our audit, DFG's senior management had determined that the Department would attempt to use its off-site storage location as an alternate processing site. This alternate processing site's primary purpose would be to support off-site IT recovery efforts. If IT processing capabilities were unavailable, access to IT resources, such as the MassOutdoors software application, spreadsheet and database applications, related data files, and other electronic documentation, would be jeopardized. DFG's off-site data storage provides a key element for the recovery of lost information on the LAN.

The objective of disaster recovery and business continuity planning is to provide reasonable assurance that mission-critical and essential functions enabled by technology can be regained within an acceptable period should a disaster cause significant disruption to computer operations. Generally accepted industry practices and standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops and maintains appropriate contingency and recovery plans, if required.

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

Recommendation:

We recommend that DFG assess its automated processing environment from a risk management and business continuity perspective and further develop and test appropriate disaster recovery and business continuity plans. We recommend that DFG further develop disaster recovery strategy elements, identify an operational alternate processing site, and test the site for its viability to support continuity of mission-critical and essential operations. We recommend that DFG ensure that its MassOutdoors application disaster recovery strategy and its Continuity of Operations Plan (COOP) are adequately reviewed, tested, and approved as an integrated disaster recovery and business continuity plan. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to DFG's operations or the overall IT environment.

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

Since the Executive Office of Energy and Environmental Affairs is DFG's oversight entity and operates the file server room where DFG's mission-critical MassOutdoors application system and data files reside, DFG needs to coordinate its disaster recovery and business continuity planning with EOEEA.

Because our audit work was completed prior to the initiation of Executive Order 510, "Enhancing the Efficiency and Effectiveness of the Executive Department's Information Technology Systems," we recommend that DFG reassess its processing and recovery requirements and continuity strategies in light of the IT consolidation efforts.

Auditee's Response

> *We largely accept the observations and recommendations regarding a Department BCP and will endeavor to work with EOEEA in the development of same.*
>
> *We'd like to make a number of specific observations regarding alternative processing sites for SPORT.*
>
> *As we noted previously, SPORT has two production servers. The SPORT production database server is in the EOEEA data center at Causeway St. and the application server is in the ITD data center in the McCormack Building.*
>
> *Our feeling is the production database server should be moved to the EOEEA data center in the Saltonstall building as soon as practicable.*

That would leave development application and database servers in the EOEEA Causeway St. data center. The development servers are basically configured the same as the production servers and can be used in production should the production machines go out of service.

Over the long run, utilization of the projected ITD data center in the western part of the state would provide greater separation and raise the probability of system survival should Boston become unavailable.

DFG (DMF and DFW but not OLE) is exploring an additional avenue of business continuity security by seeking to engage a vendor to sell its licenses and permits at which point it would leave the SPORT application altogether. The out-of-state vendor will itself have system redundancy in the form of multiple servers spread over two widely separated sites. We hope to have this plan in place in the FY11 timeframe.

Additionally, both DMF and DFW have alternative systems through which they can process licenses and permits thereby protecting the interest of the Commonwealth.

Auditor's Reply

We acknowledge that steps are underway to address disaster recovery and business continuity planning and that the Department is dependent on EOEEA and ITD. We note that recovery and contingency plans specific to the Department's operations need to be further developed. These plans should be re-evaluated if the Department were to no longer operate the SPORT application. Until appropriate disaster recovery and business continuity plans are completed, DFG remains vulnerable.

2. Prior IT Audit Results Resolved

a. IT Organization and Management

Our prior audit, No. 2007-0432-4T, disclosed that DFG did not have documented, formalized, and approved policies and procedures in place regarding IT operations. In addition, DFG did not have a formalized process for developing and maintaining an IT internal control plan, including strategic and tactical plans.

Our current audit indicated that DFG is adequately maintaining IT organization and management documents, as well as an adequate organizational structure. DFG has also had an internal control plan in effect since May 2006 that consists of financial-related controls only. However, our current audit indicated that although DFG had developed certain IT policies and procedures, the degree of documentation still needs to be enhanced for all IT functions.

Auditee's Response

We will continue to work on enhancing IT policies and procedures documentation and make sure that staff is made aware of their responsibilities in this regard. Given Exec Order 510 (IT Consolidation) we will be seeking clarification regarding the level and

type of coordination between Department and Secretariat with regard to the development and promulgation of IT policies.

b. Physical Security

Our prior audit indicated that DFG did not have documented, formalized, and approved policies and procedures in place regarding physical security controls. In addition, DFG was not maintaining visitor logs for the file server room. There were also no surveillance cameras recording activity located in or around the file server room.

Our current audit indicated that the responsibility for physical security of the file server room did not rest specifically with DFG, but rather with EOEEA. Although we found that certain physical security controls were in place, physical security controls, such as detailed security policies and procedures, needed to be strengthened. We note that DFG, in conjunction with EOEEA, now maintains a current list of employees authorized to access the file server room.

Auditee's Response

We see that the fact that responsibility for physical security of the Causeway Street EOEEA Data Center rests with EOEEA is acknowledged in this report. We will continue to cooperate with EOEEA in whatever efforts they may take to enhance physical security.

c. Environmental Protection

Our prior audit indicated that DFG did not have documented, formalized, and approved policies and procedures in place regarding environmental protection controls. General housekeeping at the file server room was poor, as there were devices plugged into extension units and wires were hung across the ceiling by butterfly clips. In addition, although there were no water detection devices, DFG did have fire suppression sprinklers; however, one of the servers was located directly below a sprinkler.

Our current audit indicated that the responsibility for environmental protection of the file server room rests with EOEEA. We note that although devices were no longer plugged into extension units, general housekeeping at the file server room still needed improving due to the improper hanging of wires on the ceiling of the file server room. In addition, although the file server room contained fire suppression sprinklers, there were still no water detection devices installed.

Auditee's Response

As the audit report points out, responsibility for environmental protection in the EOEEA Causeway Street Data Center also rests with EOEEA. As with Physical Security issues, we will continue to cooperate with EOEEA in whatever efforts they may take to enhance environmental security.

d. System Access Security

Our prior audit indicated that DFG did not have documented, formalized, and approved policies and procedures in place regarding system access security controls.

Our current audit, however, indicated that at the time of the audit, DFG has since developed sufficiently detailed policies and procedures pertaining to system access security with the intent to submit them to the DFG Commissioner for official approval.

Auditee's Response

During the previous audit, we had documented policy and procedures for system access security in place. However, they had not been formally approved by the Commissioner. For this audit, we adopted OSA's recommendation and enhanced and expanded these policies and procedures and had them formally approved by the Commissioner.

e. Inventory Control over Computer Equipment

Our prior audit indicated that DFG did not have documented, formalized, and approved policies and procedures in place regarding inventory controls of computer equipment. In addition, DFG did not have complete data fields in its IT inventory listing. DFG needed to improve its listing in such areas as tag numbers, cost amounts, dates of acquisition, and Internet protocol (IP) addresses. DFG also needed to implement sign in/out procedures for controlling the issuance of notebook computers. The IT inventory also needed to be performed on a perpetual basis and DFG needed to reconcile its inventory listing.

Our current audit indicated that DFG more sufficiently details its policies and procedures pertaining to inventory control of computer equipment and various IT-related items. However, DFG has resolved its other concerns regarding inventory controls. DFG's IT inventory listing now has the Office of the State Comptroller's required data fields, including tag numbers, cost amounts, and dates of acquisition. DFG currently performs an annual inventory of all IT-related items and maintains the inventory listing on a perpetual basis. We note that although DFG's inventory listing included all 12 notebook computers, DFG should document the procedures for recording the locations in the IT inventory.

Auditee's Response

Since the previous audit, we have strengthened our computer equipment inventory capabilities and following this audit report's recommendations, will continue to strengthen our inventory policies and procedures. However, again with reference to EO510, we will be seeking clarification regarding the level and type of coordination between Department and Secretariat with regard to the maintenance of computer equipment inventories.

Regarding surplusing, we would note we have complied with OSD Policies and Procedures including having conducted prior surplusing events and that surplus equipment stored in Department's GIS lab is reflective not of a disinclination to follow

OSD procedures, but rather of the fact that we only surplus once a year given limited staff support.

f. Virus Protection

Our prior audit indicated that DFG did not have documented, formalized, and approved policies and procedures in place regarding virus protection controls.

Our current audit indicated that DFG has documented sufficiently detailed policies and procedures pertaining to virus protection controls.

Auditee's Response

During the previous audit, we had documented policy and procedures for virus protection in place. However, they had not been formally approved by the Commissioner. For this audit, we enhanced and expanded these policies and procedures and had them formally approved by the Commissioner.

g. MassOutdoors Application System Procedures

Our prior audit indicated that DFG had implemented and was using the MassOutdoors application (formally known as the SPORT system), but had not implemented a help desk function to provide support to all users.

Our current audit indicated that DFG's help desk function supports multiple IT-related inquiries. The Department has also implemented written procedures to report, investigate, and correct all issues relating to the MassOutdoors application.

Auditee's Response

MassOutdoors has had, and continues to support a Help Desk function for all users. It is especially needed by the general public. What has improved since the last audit is our ability to track and report on issues related to the application.