

Information Technology Division

Findings on Reportable Conditions

Finding Number 15: Access to Production and Utility Libraries Should Be More Restricted

Although ITD has made a significant effort to restrict programmer access to production, some inappropriate access remains (notably four instances where a programmer has Alter Access instead of Read Access).

The alter RACF access would enable changes to be made to live applications and data. These changes could be made by bypassing the established change control process and alter the integrity or functionality of the applications. When this access was brought to the attention of the Director of Application Programmers, several programmers access was deemed inappropriate. The Director of Application Programmers has requested the removal of these programmer's access. (*Fiscal Year 1997 Single Audit Report Finding 15*)

Recommendation:

Management should continue its efforts to remove all programmers' access to production.

Department corrective action plan:

The 4 identified instances of inappropriate access will be corrected immediately. Security access policies have been reiterated to all managers in the Enterprise Applications Bureau (EAB). In addition, the EAB security administrator will now submit all requests for update or alter access to production files to the EAB Bureau Director for approval. In fiscal year 1999, a more formal, semiannual security review will be implemented.

Responsible individual: David Lewis, Acting Director

Finding Number 16: No Disaster Recovery Plan/Continuity Plan is in Place over the Communication's Room

A disaster recovery plan has been developed for the main data processing environment at the Chelsea location; however, it does not address the Communications Room. It should be noted that management is in the process of investigating a backup data center in the Milford, MA area. Management is also working with the Capital Planning & Operations (DCP) to fund a project to upgrade the MAGNET Frame Relay network control center on the McCormack Building's 8th floor. (*Fiscal Year 1997 Report*)

*Finding 16)***Recommendation:**

Management should develop a formal disaster recovery plan and business continuity plan in line with the current plans developed at the Chelsea location.

Department Corrective Action Plan:

ITD and DCP are in the design and planning stages of upgrading the current Network Control Center with additional electrical power, backup generator and cooling. This is scheduled to be complete by end of fiscal year 1999.

The data center is in the final phase of preparing an RFR for disaster recovery services. A byproduct of this effort was the review of the communication requirements for the data center. The long-term recommendation will be the splitting of the Ashburton network into three parts forming a communications triangle. Ashburton, Chelsea and the future ITD recovery site in Milford make up the proposed triangle. Users of a failing part of the triangle will be rerouted to the data center via the other two sections.

This long-term recommendation will be published by the data center mid fall 1998.

Responsible individual: David Lewis, Acting Director

Finding Number 17: Business Continuity Planning

Information Technology Division (ITD) is in the process of completing a Business Impact Analysis to determine their business continuation requirements in emergency circumstances. However, a formal business continuity plan has not been developed nor communicated to employees and key stakeholders.

The primary goals for business continuity include minimizing or eliminating threats, minimizing immediate damage and losses, ensuring that critical services and processes can continue, ensuring restoration of your work force, facilities and equipment in a timely fashion, and ensuring the timely business resumption for essential business functions. The Business Impact Analysis (BIA) is the component that drives all business continuity activities and expenditures. It assesses the potential operational and financial impact of a disruption over time. The technical and logistical aspects of continuity planning are developed and implemented based on business requirements for availability and recovery. (*Fiscal Year 1996; 1997 Report Finding 17*)

Recommendation:

We recommend that ITD should continue with its BIA in order to educate its clients to quantify the exposure and problems that would develop should a business interruption occur. Once the comprehensive BIA is completed, management should continue the process of Business Continuity Planning by directing the resources to focus on the identified risks.

Department corrective action plan:

ITD has solicited responses (Business Impact Analysis) from the various agencies that utilize the data center. The responses have been summarized and weighted resulting in the identification of 102 distinct applications. The final step will result in a published list of critical applications that must be recoverable in the event of a disaster. A technical requirements list will be developed and used as the basis for contracting for recovery services.

ITD has educated its clients during the gathering of this material and will continue to do so as we move forward in this effort. Each application owning Agency will be contacted and educated in the need for a recovery plan as well as testing it.

Responsible individual: David Lewis, Acting Director

Finding Number 18: Statewide Information Security Architecture

Although the CIO has authorized the Information Technology Division's (ITD) Operations Committee, composed of the directors of ITD's principal operations bureaus, with the responsibility for assessing and developing statewide security policies and procedures, the State has not yet commenced the implementation and enforcement phase of the information security architecture. The Information Security Policy and Architecture will provide consistent guidance and direction to the various data centers and LANs throughout the Commonwealth. There are twelve data centers and numerous LANs currently in use in the Commonwealth and there are plans to expand the utilization of information technology to support the operations of the State.

Standard security procedures across complex computing environments, such as the Commonwealth, would contribute to lower levels of administration and overhead costs, create efficiencies, and could result in fewer security exposures. Some of the critical areas to be addressed in an Information Security Policy include: assignment of access privileges, annual security reviews, monitoring and audit trails, proper use of IDs and passwords, virus protection, use of the Internet and exposure to outside threats. It should be noted that the ITD's Operations Committee has contracted outside consulting agencies to assist in the assessment and development of statewide security policies and procedures. (*Fiscal Year 1996; 1997 Report Finding 9*)

Recommendation:

We recommend that the Commonwealth continue its efforts in the assessment and development of the Statewide Security Architecture and Policy and implement the architecture across the Commonwealth as soon as possible.

Department Corrective Action Plan:

ITD will continue to address information security requirements on several fronts, regularly assessing costs and risks, and making constant adjustments and improvements. The efforts completed in fiscal year 1998 played a critical role on establishing a foundation for moving ahead with a statewide information security architecture.

ITD is currently undertaking a major strategic planning effort focused on information security. This initiative involves representatives from all ITD's operations bureaus, as well as people from ITD's strategic planning bureau, Internet services bureau, network applications bureau and Office of General Counsel. This information security task force will work with the statewide Information Technology Coordinating Council to involve a diverse group of IT-reliant agencies. Two specific activities planned for fiscal year 1999 will be to retain expert consultants to conduct a security assessment, with specific focus on network security issues, and to develop a security policy for the Commonwealth of Massachusetts.

Responsible individual: David Lewis, Acting Director

Information Technology Division

Findings Not Repeated From Prior Years

1. Some terminated employees user IDs remained active and some user IDs were inactive but remained on the system. The Division's security data base was updated to allow for the distinction between employee and consultant, including an expiration date. Testing of a sample of terminated employees was performed to ensure that access was removed in a timely manner. (*Fiscal Year 1997 Report Finding 14*)
2. Security over remote access appeared to be inconsistent across access points to the network. The Division engaged a security vendor to assess the security of the firewall deployment and a vendor to provide firewall vulnerability detection software that will allow the Division to perform its own audits of firewall security. (*Fiscal Year 1997 Report Finding 18*)

[Table of Contents](#)

[Next](#)

[Privacy Policy](#)

Any questions? Send e-mail to: comptroller.info@state.ma.us.

Copyright 1999-2001, Massachusetts Office of the Comptroller, all rights reserved.