PERFORMANCE AUDIT
OF THE

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS

December 2000

51-590-00

EXECUTIVE DIGEST

AUTOMATED INFORMATION SYSTEMS

INTRODUCTION

This report, issued in December 2000, contains the results of our performance audit* of the Automated Information Systems, Department of Military and Veterans Affairs.

AUDIT PURPOSE

This performance audit was conducted as part of the constitutional responsibility of the Office of the Auditor General. Performance audits are conducted on a priority basis related to the potential for improving effectiveness* and efficiency*.

BACKGROUND

The Directorate of Information Management (DOIM) provides computer services to the Department's headquarters. DOIM reports to the Department's Office of the Director and the Adjutant General. The mission* of DOIM is to provide the Department's headquarters with reliable voice and data communications services that meet or exceed service levels established by the director. These include wide area network* (WAN) connectivity, network management, electronic messaging administration, and voice systems. As of March 31, 2000, DOIM had 7 State employees. In addition, DOIM had 20 federal employees responsible for the administration and maintenance of the Department's federal networks.

\

* *See glossary at end of report for definition.*

The Grand Rapids Home for Veterans and the D.J. Jacobetti Home for Veterans are responsible for providing domiciliary care* and nursing care* to veterans of the State and to widows, widowers, spouses, former spouses, and parents of State veterans.

The Homes each have an information systems unit that is responsible for providing computer services to the Home. Some of the services provided include purchasing, installing, and maintaining hardware and software and managing the Homes' local area networks* (LANs).

AUDIT OBJECTIVES AND CONCLUSIONS

Audit Objective: To assess the effectiveness of the Department's LANs and end-user computing (EUC) in providing reliable and secure information.

Conclusion: The Department's LANs and EUC were reasonably effective in providing reliable and secure information. However, we noted reportable conditions* related to a security program, LAN access controls, LAN backup and recovery controls, LAN administrator training, and policies and procedures (Findings 1 through 5).

Audit Objective: To assess internal control* and the effectiveness of input, processing, and output controls over the Department's automated information systems.

Conclusion: Internal control over the Department's automated information systems was reasonably effective. However, we noted a reportable condition related to system application controls (Finding 6).

AUDIT SCOPE AND METHODOLOGY

Our audit scope was to examine the information processing and other records of the Department

* *See glossary at end of report for definition.*

of Military and Veterans Affairs' automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Our methodology included examination of the Department's information processing and other records for the period August 1999 through March 2000. Our methodology also included identifying the Department's automated information systems and performing a risk assessment of each system. We used this assessment to determine the systems to audit and the extent of our detailed analysis and testing. We performed an assessment of internal control pertaining to (a) general controls for the Department's LAN, which included network administration, physical security, access, and management controls; and (b) application controls for the Accumax System*, MDI System*, Census System*, and Finance System*, which included data input, data processing, and data output controls.

AGENCY RESPONSES

Our audit report contains 6 findings and 6 corresponding recommendations. The Department's preliminary response indicated that it agreed with all of the findings.

* *See glossary at end of report for definition.*

This page left intentionally blank.

December 26, 2000

Major General E. Gordon Stump, Director
Department of Military and Veterans Affairs
2500 South Washington Avenue
Lansing, Michigan

Dear General Stump:

This is our report on the performance audit of the Automated Information Systems, Department of Military and Veterans Affairs.

This report contains our executive digest; description of agency; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This page left intentionally blank.

TABLE OF CONTENTS

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF MILITARY AND VETERANS AFFAIRS

INTRODUCTION

COMMENTS, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Directorate of Information Management (DOIM)

DOIM provides computer services to the Department of Military and Veterans Affairs' headquarters. DOIM reports to the Department's Office of the Director and the Adjutant General. The mission of DOIM is to provide the Department's headquarters with reliable voice and data communications services that meet or exceed service levels established by the director. These include wide area network (WAN) connectivity, network management, electronic messaging administration, and voice systems. As of March 31, 2000, DOIM had 7 State employees. In addition, DOIM had 20 federal employees responsible for the administration and maintenance of the Department's federal networks.

The Grand Rapids Home for Veterans and the D.J. Jacobetti Home for Veterans are responsible for providing domiciliary care and nursing care to veterans of the State and to widows, widowers, spouses, former spouses, and parents of State veterans.

The Homes each have an information systems unit that is responsible for providing computer services to the Home. Some of the services provided include purchasing, installing, and maintaining hardware and software and managing the Homes' local area networks. The Accumax System, MDI System, Census System, and Finance System are information processing systems that the Homes use to process and store residents' clinical and accounting information.

Accumax System

In January 2000, the Grand Rapids Home for Veterans completed its implementation of the Accumax System. The Accumax System is an integrated clinical and accounting system. Staff use this System for admissions, daily census reporting, resident assessments and care plans, resident accounting, and reporting. As of March 2000, the System contained comprehensive information for approximately 700 residents.

MDI System

The D.J. Jacobetti Home for Veterans purchased and implemented the MDI System in 1997. The MDI System is the Home's comprehensive health care tracking system. Staff use this System for admissions, resident assessments and care plans, and

reporting. As of March 2000, the System contained comprehensive information for approximately 200 residents.

Census System

The D.J. Jacobetti Home for Veterans' information systems staff designed and developed the Census System. The System tracks each resident's attendance and location within the Home and generates monthly billing information for the U.S. Department of Veterans Affairs.

Finance System

The D.J. Jacobetti Home for Veterans' information systems staff also designed and developed the Finance System. The Home implemented the Finance System in November 1998. The System accounts for residents' funds held in trust by the Home. The System generates each resident's statement of account on a monthly basis. During fiscal year 1998-99, the System processed $4.4 million in receipts and $4.4 million in payments for approximately 200 residents.

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit of the Automated Information Systems, Department of Military and Veterans Affairs, had the following objectives:

1. To assess the effectiveness of the Department's local area network (LAN) and end-user computing (EUC) in providing reliable and secure information.

2. To assess internal control and the effectiveness of input, processing, and output controls over the Department's automated information systems.

Audit Scope

Our audit scope was to examine the information processing and other records of the Department of Military and Veterans Affairs' automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Department's information processing and other records for the period August 1999 through March 2000. Our work was performed from August 1999 through April 2000. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We identified the Department's automated information systems and performed a risk assessment of each system to identify the systems with the highest risk. Our risk assessment considered the critical nature of the information processed through each system. We used this assessment to determine the systems to audit and the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

We collected background information about the Department's automated information systems. We performed an assessment of internal control pertaining to (a) general controls for the Department's LAN, which included network administration, physical security, access, and management controls; and (b) application controls for the Accumax System, MDI System, Census System, and Finance System, which included data input, data processing, and data output controls:

a. Effectiveness of General Controls:

We analyzed controls over the management and operation of the Department's LAN.

We observed and assessed the security of the LAN, including physical security, backup, and access controls.

b. Internal Control Over Automated Information Systems:

We evaluated controls over the access and use of the Accumax, MDI, Census, and Finance Systems.

We assessed and documented internal control over data input, data processing, and data output of the Accumax, MDI, Census, and Finance Systems. Also, we conducted tests to determine whether the controls were working as intended.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

Agency Responses

Our audit report contains 6 findings and 6 corresponding recommendations. The Department's preliminary response indicated that it agreed with all of the findings.

The agency preliminary response which follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the Department of Management and Budget Administrative Guide procedure 1280.02 require the Department of Military and Veterans Affairs to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF LOCAL AREA NETWORKS (LANs) AND END-USER COMPUTING (EUC)

COMMENT

Audit Objective: To assess the effectiveness of the Department of Military and Veterans Affairs' LANs and EUC in providing reliable and secure information.

Conclusion: The Department's LANs and EUC were reasonably effective in providing reliable and secure information. However, we noted reportable conditions related to a security program, LAN access controls, LAN backup and recovery controls, LAN administrator training, and policies and procedures.

FINDING

1. Security Program

The Department had not established a comprehensive information systems security program.

Executive management has the responsibility to ensure the security and integrity of agency information systems resources. A comprehensive security program should include detailed policies and procedures for safeguarding all information system resources. The General Accounting Office's Federal Information System Controls Audit Manual (issued in January 1999) states that a comprehensive security program should include:

a. Periodic risk assessments.

b. A documented entitywide security program, security management structure, and clearly assigned security responsibilities.

c. Effective security related personnel policies.

d. A plan to monitor the security program's effectiveness and to make changes as needed.

One method of effectively addressing information systems security issues is by appointing a security officer as required by Department of Management and Budget (DMB) Administrative Guide procedure 1310.02. The Department had assigned the network security function to the managers responsible for administering the networks. Although, the network administrators have a role to play in maintaining the security of network resources, the responsibility for overall network security should be independent from its administration. An independent security officer should monitor system access and educate users about the importance of information systems security. Security officer duties also include establishing a security program, developing and enforcing security policies and procedures, and monitoring system-recorded security activities and violations.

The Department's lack of a comprehensive security program resulted in a number of security weaknesses, which are addressed in this report (Findings 2 through 5).

RECOMMENDATION

We recommend that the Department establish a comprehensive information systems security program.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has developed a comprehensive security program and has implemented Departmentwide policies and procedures. The Department also informed us that it will appoint a security officer in accordance with DMB Administrative Guide procedure 1310.02.

FINDING

2. LAN Access Controls

The Department had not established complete controls over access to data and application program files on the LANs. Establishing additional controls would help ensure that only authorized users have access to the data and applications needed to perform their assigned duties.

We reviewed LAN file server security and noted weakness relating to: usercodes and passwords, sign-on attempts, multiple log-ons, inactive network connections, computer security agreements, LAN administrator usercodes and administrative access rights, monitoring, and access to network resources.

RECOMMENDATION

We recommend that the Department establish complete controls over access to data and application program files on the LANs.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding. The Department informed us that it has established an acceptable use policy and an information systems security policy at all Department sites.

FINDING

3. LAN Backup and Recovery Controls

The Department had not established complete backup and recovery controls. Improving backup and recovery controls would help ensure that the LAN and critical application and data files can be restored in the event of a disaster.

Our review of backup and recovery controls disclosed:

a. The Department did not retain backup tapes for a sufficient period of time. The D.J. Jacobetti Home for Veterans retained backup tapes for only the most recent 60 days of activity, the Grand Rapids Home for Veterans retained backup tapes for 180 days, and Department headquarters retained backup tapes for 365 days. Increasing the retention period would improve the Department's ability to reconstruct critical files and data.

b. The Department did not store current copies of its LAN application and database backup files off-site. At Department headquarters and both Homes, backup tapes were stored in the server room. Rotating backup tapes to an off-site location would help ensure the recovery of files in the event of an on-site disaster.

c. The Department had not fully completed and tested a written plan for recovering the LANs from backup files and restoring data and programs in the event of a disaster. Data and programs can be lost through human error, equipment malfunction, and natural disasters. Without adequate planning and testing, restoring backup files and recovering from a disaster could be extremely costly and time consuming, if not impossible, and could significantly impair Department operations.

As part of its year 2000 contingency planning, the Department developed a continuity of operation plan to identify risks to the LANs and to provide guidance for contingency operations. The Department could expand its continuity of operation plan to provide the basis for a comprehensive disaster recovery plan.

RECOMMENDATION

We recommend that the Department establish complete backup and recovery controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has developed backup and recovery controls for its LANs.

FINDING

4. LAN Administrator Training

The Department had not established a continuing education policy for LAN administrators.

In 1999, the Department completed the conversion of its LANs to a new network operating system. The network operating system provides various security features which help secure the LANs and their data. In addition, the LAN software provides additional utilities to help the administrator manage the LANs.

The Grand Rapids Home for Veterans' and the D.J. Jacobetti Home for Veterans' LAN administrators had not received training on the new network operating

system. As a result, not all administrators were aware of the security features and utilities available through the LAN software. This contributed to access control weaknesses (Finding 2).

Establishing a continuing education policy would help ensure that LAN administrators maintain existing skills and obtain new skills as information technology changes.

RECOMMENDATION

We recommend that the Department establish a continuing education policy for LAN administrators.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it will develop a continuing education policy for information technology employees. The Department also informed us that it has initiated a self-study program and a computer-based training program to meet short-term training needs.

FINDING

5. Policies and Procedures

The Department had not developed comprehensive policies and procedures for LAN administration and EUC.

We noted:

a. The Department had not developed and implemented comprehensive LAN administration policies and procedures, including those for network installation, hardware and software configuration, system performance, and problem identification and tracking. In addition, the Grand Rapids Home for Veterans and the D.J. Jacobetti Home for Veterans had not clearly defined the roles and responsibilities of the LAN administrators.

b. The Department had not developed and implemented comprehensive EUC policies and procedures addressing general security, physical security, software and data access security, and network security. Both Homes and Department headquarters had developed or were developing EUC policies

and procedures. However, the policies and procedures were not uniform and did not consistently address all security issues. DMB Administrative Guide procedure 1310.02 requires all departments to develop comprehensive EUC policies, procedures, and guidelines.

Lack of documented policies and procedures could weaken security over the Department's LANs and EUC. For example, users may be unclear or misunderstand their responsibilities and administrators may improperly implement or inconsistently apply controls.

RECOMMENDATION

We recommend that the Department develop comprehensive policies and procedures for LAN administration and EUC.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has taken steps to comply with the recommendation. Since our audit, the Department has updated or issued six policies related to LAN administration and EUC.

INTERNAL CONTROL OVER AUTOMATED INFORMATION SYSTEMS

COMMENT

Audit Objective: To assess internal control and the effectiveness of input, processing, and output controls over the Department's automated information systems.

Conclusion: Internal control over the Department's automated information systems was reasonably effective. However, we noted a reportable condition related to system application controls.

FINDING

6. System Application Controls

The Department had not established complete application control procedures to ensure the security and integrity of computer data and records.

We reviewed input, processing, and output controls over the Accumax, MDI, Census, and Finance Systems. We noted:

a. The Department had not established complete control procedures to prevent unauthorized access and use of the Accumax, MDI, and Finance Systems. Improved access controls would help provide accountability for transactions processed by the applications.

b. The Department had not established controls to provide system audit trails for the Accumax, MDI, Census, and Finance Systems. The design of these systems did not include an audit trail to assist in the reconstruction of data files and to enable management to identify the originator of the transactions. An audit trail would record the date, time, usercode, and data changed for each transaction.

c. The Department did not enforce controls designed to ensure the accuracy and completeness of information produced by the MDI System. The MDI System produces each resident's minimum data set (MDS) assessment and care plan. The MDS assessment is a standardized and comprehensive assessment of a resident's functional capabilities and helps the staff to identify health problems. Our review disclosed:

   (1) The D.J. Jacobetti Home for Veterans did not require its staff to error check and lock a resident's completed MDS assessment. The system has error checking capabilities to ensure that the assessment satisfies system edits. After passing all edits, the assessment should be locked to prevent subsequent changes to the assessment. Our analytical review identified 94 (40%) of 236 assessments that had not been error checked. In addition, agency staff informed us that they did not lock the assessments.

(2) The D.J. Jacobetti Home for Veterans did not require all staff who completed a portion of the MDS assessment to certify its accuracy. Agency staff informed us that only the registered nurse coordinator signs and certifies the MDS assessment. To help ensure that the assessment accurately reflects the resident's condition, the Home should require each individual team member who completes a portion of the assessment to sign and certify its accuracy.

Validation of MDS assessments would help ensure that residents' care plans accurately reflect their health care needs.

d. The Department had not established sufficient controls over changes to MDI data. The D.J. Jacobetti Home for Veterans' LAN administrator purged MDI data without user involvement. The LAN administrator's duties included maintaining network and system performance. When necessary, to improve performance, the administrator would purge the MDI data tables of duplicate and deceased resident records. However, the MDI System's users are ultimately responsible for the integrity of its data. As such, they should be involved in the process of maintaining information on data tables. Clearly defining the responsibilities of users and the network administration would help ensure proper controls over database maintenance and data integrity.

RECOMMENDATION

We recommend that the Department establish complete application control procedures to ensure the security and integrity of computer data and records.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that, where possible, it has identified and corrected weaknesses. In addition, the Department informed us that it has approached its software vendors for technical support to address the outstanding access control limitations. The Department expects future releases of the software to have enhanced security controls.

Glossary of Acronyms and Terms

Accumax System	A computer system used by the Grand Rapids Home for Veterans to process and store residents' clinical and accounting records.
Census System	A computer system used by the D.J. Jacobetti Home for Veterans to track its residents' locations.
DMB	Department of Management and Budget.
DOIM	Directorate of Information Management.
domiciliary care	Care for self-sufficient individuals who are able to adequately perform all activities of daily living.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical for the amount of resources applied or minimizing the amount of resources required to attain a certain level of outputs or outcomes.
EUC	end-user computing.
Finance System	A computer system used by the D.J. Jacobetti Home for Veterans to account for residents' funds held in trust by the Home.
internal control	The management control environment, management information system, and control policies and procedures established by management to provide reasonable assurance that goals are met; that resources are used in compliance with laws and regulations; and that valid and

	reliable performance related information is obtained and reported.
local area network (LAN)	A group of computers connected to each other over a small geographical area, such as a building or office, for the purpose of sharing hardware, software, and information.
MDI System	A computer system used by the D.J. Jacobetti Home for Veterans to process and store residents' clinical information.
MDS	minimum data set.
mission	The agency's main purpose or the reason the agency was established.
nursing care	Care for individuals who need assistance with daily living activities.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
reportable condition	A matter coming to the auditor's attention that, in the auditor's judgment, should be communicated because it represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
wide area network (WAN)	A group of computers connected to each other over a large geographical area, such as the State, for the purpose of sharing hardware, software, and information.