PERFORMANCE AUDIT

OF THE

LAW ENFORCEMENT INFORMATION NETWORK AND CRIMINAL JUSTICE DATA CENTER

MICHIGAN DEPARTMENT OF STATE POLICE

December 1997

55-591-96

EXECUTIVE DIGEST

LAW ENFORCEMENT INFORMATION NETWORK AND CRIMINAL JUSTICE DATA CENTER

INTRODUCTION

This report, issued in December 1997, contains the results of our performance audit* of the Law Enforcement Information Network* (LEIN) and the Criminal Justice Data Center (CJDC), Michigan Department of State Police (MSP).

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

Michigan's LEIN is a Statewide computerized information system that enables participating law enforcement agencies to access and/or modify stored information. LEIN includes data bases containing sensitive criminal and law enforcement information accessible by remote terminals throughout the State. The LEIN data files contain a computerized index of documented criminal justice information concerning crimes and criminals of Statewide, as well as national, interest. LEIN provides access to the National Law Enforcement Telecommunications System* (NLETS), the National Crime Information Center* (NCIC), and various State data bases.

* *See glossary on page 33 for definition.*

CJDC is responsible for access to and management of LEIN. CJDC manages this system in accordance with the regulations imposed by the LEIN Policy Council* and the Federal Bureau of Investigation (FBI), U.S. Department of Justice.

CJDC is also responsible for computer-related processing services for MSP. CJDC provides services to departmental management in the form of automated systems design, computer program development, and data processing.

CJDC was appropriated $11.8 million for fiscal year 1996-97 and was authorized 93 full-time equated positions as of October 1, 1996.

AUDIT OBJECTIVES AND CONCLUSIONS

Audit Objective: To assess the reliability of LEIN controls in ensuring accurate, complete, timely, and secure information for law enforcement agencies.

Conclusion: Our assessment disclosed that LEIN controls were reasonably reliable in ensuring accurate, complete, timely, and secure information for law enforcement agencies. However, we noted four reportable conditions* regarding strategic plans, LEIN audits, timeliness of records, and authentication* of LEIN users (Findings 1 through 4).

Audit Objective: To assess the effectiveness of CJDC's internal control structure in providing reliable and secure information.

Conclusion: Our assessment disclosed that CJDC's internal control structure was reasonably effective in providing reliable and secure information. However, we

** See glossary on page 33 for definition.*

noted 11 reportable conditions related to CJDC's internal control structure over the data center. These conditions involved system access controls and security administration, separation of duties, network security, and disaster recovery and file backup (Findings 5 through 8). The conditions also involved computer room access, user identification codes and station controls, production disk pack controls, and database security (Findings 9 through 12). In addition, conditions involved documentation standards, tape control procedures, and output distribution (Findings 13 through 15).

AUDIT SCOPE AND METHODOLOGY

Our audit scope was to examine the Law Enforcement Information Network records and the data processing and other records of the Criminal Justice Data Center. 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.

We collected background information about LEIN and CJDC and obtained an understanding of the internal control structure. We examined records for the period October 1994 through May 1997, observed activities, and conducted interviews with agency and law enforcement personnel regarding LEIN application controls, management, security, systems software, system development, operations, and end-user computing. We then performed analysis and testing and verified the effectiveness of the internal control structure. Our final phase was to evaluate and report on the results of our data gathering phase and the detailed analysis and testing phase.

AGENCY RESPONSES AND PRIOR AUDIT FOLLOW-UP

Our audit report contains 15 findings and 25 corresponding recommendations. The agency's preliminary response indicated that MSP has complied or will comply with all of the recommendations.

We repeated 14 of the 20 prior audit recommendations included within the scope of our current audit.

Colonel Michael D. Robinson, Director
Michigan Department of State Police
714 South Harrison
East Lansing, Michigan

Dear Colonel Robinson:

This is our report on the performance audit of the Law Enforcement Information Network and the Criminal Justice Data Center, Michigan Department of State Police.

This report contains our executive digest; description of agency; audit objectives, scope, and methodology and agency responses and prior audit follow-up; 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

LAW ENFORCEMENT INFORMATION NETWORK AND CRIMINAL JUSTICE DATA CENTER MICHIGAN DEPARTMENT OF STATE POLICE

INTRODUCTION

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

Michigan's Law Enforcement Information Network (LEIN) is a Statewide computerized information system that enables participating law enforcement agencies to access and/or modify stored information. LEIN includes data bases containing sensitive criminal and law enforcement information accessible by remote terminals throughout the State. The LEIN data files contain a computerized index of documented criminal justice information concerning crimes and criminals of Statewide, as well as national, interest. LEIN provides access to the National Law Enforcement Telecommunications System (NLETS), the National Crime Information Center (NCIC), and various State data bases.

The Criminal Justice Data Center (CJDC) is responsible for access to and management of LEIN. CJDC manages this system in accordance with the regulations imposed by the LEIN Policy Council and the Federal Bureau of Investigation (FBI), U.S. Department of Justice.

CJDC is also responsible for computer-related processing services for the Michigan Department of State Police. CJDC provides services to departmental management in the form of automated systems design, computer program development, and data processing.

CJDC was appropriated $11.8 million for fiscal year 1996-97 and was authorized 93 full-time equated positions as of October 1, 1996.

Audit Objectives, Scope, and Methodology and Agency Responses and Prior Audit Follow-Up

Audit Objectives

Our performance audit of the Law Enforcement Information Network (LEIN) and the Criminal Justice Data Center (CJDC), Michigan Department of State Police (MSP), had the following objectives:

1. To assess the reliability of LEIN controls in ensuring accurate, complete, timely, and secure information for law enforcement agencies.

2. To assess the effectiveness of CJDC's internal control structure in providing reliable and secure information.

Audit Scope

Our audit scope was to examine the Law Enforcement Information Network records and the data processing and other records of the Criminal Justice Data Center. 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

To accomplish our audit objectives, our audit methodology included the following phases:

1. Data Gathering Phase

   We collected background information about LEIN and CJDC and obtained an understanding of the internal control structure. We examined records for the period October 1994 through May 1997, observed activities, and conducted interviews with agency and law enforcement personnel regarding LEIN application controls, management, security, systems software, system development, operations, and end-user computing.

2. Detailed Analysis and Testing Phase

   We performed analysis and testing and verified the effectiveness of the internal control structure.

3. Evaluation and Reporting Phase

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

Agency Responses and Prior Audit Follow-Up

Our audit report contains 15 findings and 25 corresponding recommendations. The agency's preliminary response indicated that MSP has complied or will comply with all of the recommendations.

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 Complied Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require MSP to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

We repeated 14 of the 20 prior audit recommendations included within the scope of our current audit.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

LAW ENFORCEMENT INFORMATION NETWORK (LEIN)

COMMENT

Audit Objective: To assess the reliability of LEIN controls in ensuring accurate, complete, timely, and secure information for law enforcement agencies.

Conclusion: Our assessment disclosed that LEIN controls were reasonably reliable in ensuring accurate, complete, timely, and secure information for law enforcement agencies. However, we noted four reportable conditions regarding strategic plans, LEIN audits, timeliness of records, and authentication of LEIN users.

FINDING

1. Strategic Plans

The Michigan Department of State Police (MSP) needs to modify its strategic plans to help improve the overall effectiveness of LEIN.

MSP established plans and goals for LEIN to provide accurate and timely criminal justice information which is readily available to law enforcement agencies. While LEIN was generally effective in meeting these goals, we did note problems with the accuracy and timeliness of LEIN records (Findings 2 and 3). MSP has attempted to address these problems through the use of field audits by the LEIN Field Services Section. It has also attempted to encourage court administrators to assume greater responsibility for the entry of LEIN information.

While MSP is responsible for the operation of the LEIN system, the local law enforcement agencies and courts enter the information into the system and are responsible for ensuring the accuracy of the information. A major cause for information on LEIN being inaccurate and untimely was a lack of applied resources at all levels required to maintain the system. To impact the accuracy and timeliness of LEIN records, MSP will need to revise its strategic plans. To be

effective, MSP's revised approach will need to include obtaining input from system users to help define ways to increase the accuracy and timeliness of information while minimizing required resources.

Inaccurate or untimely LEIN records could jeopardize the safety of the public and law enforcement personnel and could also result in possible litigation.

RECOMMENDATION

We recommend that MSP modify its strategic plans, in conjunction with system users, to help improve the overall effectiveness of LEIN.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendation. MSP informed us that, while recognizing that courts and local agencies are responsible for and do maintain these records, MSP should and will focus attention on this problem in its strategic plans. MSP also informed us that it has adopted a Vision Statement that will encourage increased awareness of its criminal justice partners. MSP will use this vision to encourage the courts and local police agencies to address accuracy and timeliness. In addition, MSP informed us that it will work through the LEIN Policy Council, LEIN training, and LEIN News Bulletins to bring awareness to this problem.

FINDING

2. LEIN Audits

The LEIN Field Services Section did not comply with audit requirements and procedures. Our review of the Section's audits of procedures and records of terminal agencies* or "of agencies with terminals" disclosed:

a. The Section did not audit each terminal agency at least once every two years. The National Crime Information Center (NCIC) requires a biennial audit of all terminal agencies. The State had over 750 terminal agencies; however, the Section audited only 463 (62%) terminal agencies from October 1994 through May 1997.

* *See glossary on page 33 for definition.*

Although the field audits can be an effective tool to help ensure the effectiveness of the system, the Section only had one full-time auditor to conduct agency audits. This prevented the Section from completing all required audits and audit procedures. This also contributed to problems with the accuracy of system records.

For example, our examination of LEIN field reviews conducted by the Section from July 1995 through October 1996 disclosed that entering agencies did not properly complete record validations. Of 659 records reviewed by the Section, 137 (21%) were invalid or contained errors and had to be canceled from the system:

Record Type	Number Reviewed	Number Canceled	Error Rate
Warrants	331	22	7%
Vehicles	253	70	28%
Missing Persons	67	41	61%
Injunctive Orders	8	4	50%
Total	659	137	21%

The proper validation of these records would have eliminated most, if not all, of the errors. The Section issued reports to law enforcement agencies to communicate lack of compliance with LEIN policies and procedures. However, the Section was unable to audit all law enforcement agencies and did not conduct audits frequently enough to ensure the continued compliance with policies and procedures.

b. The Section did not complete all relevant audit procedures. For example, Section audit policies and procedures state that agency audits will concentrate on the validity, accuracy, completeness, and timeliness of records. However, the auditors did not conduct tests of the timeliness of entries in accordance with the audit procedures.

c. The Section did not employ statistical sampling techniques. For example, the auditors did not take into consideration factors such as expected error rates,

required precision*, or acceptable confidence levels* when determining sample sizes. The auditors should use statistical sampling techniques to help ensure that they develop appropriate sample sizes and reach valid conclusions.

RECOMMENDATION

We recommend that the LEIN Field Services Section comply with audit requirements and procedures.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendation and informed us that it is increasing its audit staff from one to three persons.

FINDING

3. Timeliness of Records

MSP needs to expand its communication efforts with court administrators to ensure the timely entry and removal of LEIN records. Our review of the timeliness of records disclosed:

a. Law enforcement agencies did not always enter records into LEIN in a timely manner. We selected a random sample of 70 warrants dealing with serious felonies, such as murder, rape, and kidnapping. We found that law enforcement agencies entered 38 (54%) of the warrants 4 days or more after their issuance. Law enforcement agencies entered 14 (37%) of the 38 warrants 15 or more days after the warrant were issued. NCIC officials stated that law enforcement agencies should enter warrants into the system no more than 3 days following their issuance.

Law enforcement agencies indicated that some delays resulted when courts did not provide them with the warrants in a timely manner. Also, law enforcement agencies did not always have available resources or time to commit to entering warrants.

** See glossary on page 33 for definition.*

Law enforcement agencies need to enter warrants in a timely manner to ensure that necessary information is available to law enforcement personnel as soon as possible. Information not entered in a timely manner could hinder the performance of law enforcement personnel and possibly jeopardize their safety.

b. Law enforcement agencies did not always request courts to recall old warrants in a timely manner. We determined that approximately 54,000 (7%) of 765,000 warrants were 10 years or older. Courts are responsible for recalling warrants, but law enforcement agencies need to inform the courts about warrants that appear to be old and not likely to be enforced.

Old records, which will not be enforced, should be removed from the system in a timely manner to help ensure system efficiency. Not removing such records from the system in a timely manner could possibly result in inappropriate apprehensions and civil liability suits against law enforcement agencies.

MSP has attempted, without success, to encourage courts to take on greater responsibility for the entry of warrants. However, it should expand these efforts through means such as the LEIN Policy Council, the LEIN News Bulletins, and continual communication with court administrators.

RECOMMENDATION

We recommend that MSP expand its communication efforts with court administrators to ensure the timely entry and removal of LEIN records.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendation and informed us that it will work with the courts and local law enforcement agencies to bring attention to this problem. In addition, MSP informed us that it will conduct a review of the timeliness issues with users and will develop a plan to correct the problem by October 1, 1998.

FINDING

4. Authentication of LEIN Users

MSP had not developed control procedures for the authentication of LEIN users who did not need immediate access to the system.

Authentication is a process to identify users and access rights to a system. Most systems require user identification codes and passwords for authentication. Some users of LEIN, such as police officers, require immediate access to the system. MSP does not require or use authentication methods for LEIN because such methods could adversely affect police officers' access to the system and possibly their safety.

However, other users of the system do not require immediate system access. As such, control procedures requiring authentication of these users would not jeopardize the safety of law enforcement personnel. MSP should formally define which users should be subject to authentication controls based on safety and practicality considerations. Written procedures and authentication requirements would help to restrict access and establish better audit trails of system use.

Allowing all users to access LEIN without proper authentication increases the risk of improper access and use of LEIN data.

RECOMMENDATION

We recommend that MSP develop control procedures for the authentication of LEIN users who do not need immediate access to the system.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendation. MSP informed us that the FBI relies on a user agreement with MSP in regard to security and does not require user authentication at the transaction level. Similarly, MSP employs user agreements with users of the LEIN system. However, MSP informed us that it will review the area of access controls and assess the need for enhanced control procedures. MSP also informed us that a security officer position will be established to develop a recommendation in this area.

CRIMINAL JUSTICE DATA CENTER (CJDC)

COMMENT

Audit Objective: To assess the effectiveness of CJDC's internal control structure in providing reliable and secure information.

Conclusion: Our assessment disclosed that CJDC's internal control structure was reasonably effective in providing reliable and secure information. However, we noted 11 reportable conditions related to CJDC's internal control structure over the data center. These conditions involved system access controls and security administration, separation of duties, network security, and disaster recovery and file backup. The conditions also involved computer room access, user identification codes and station controls, production disk pack controls, and database security. In addition, conditions involved documentation standards, tape control procedures, and output distribution.

FINDING

5. System Access Controls and Security Administration

CJDC had not developed complete control procedures over system access and security administration. We noted the following weaknesses:

a. CJDC did not restrict access to the system software program, Command and Edit (CANDE), to authorized developmental staff. Developmental staff used CANDE to develop, compile, and execute computer programs. Allowing nondevelopmental users access to CANDE increases the risk of inappropriate changes to computer programs. Restricting access to CANDE would help ensure computer program integrity.

In our prior report, we recommended that CJDC improve system access controls by restricting CANDE access to authorized developmental staff. CJDC agreed with our recommendation but had not complied with it.

b. MSP did not delete usercodes of employees who had either terminated employment or transferred. Our review of 40 usercodes identified 17 (43%)

that belonged to former employees. Not removing access to former employees could result in unauthorized transactions.

c. CJDC allowed access to its operating system with passwords as short as one character. Passwords should be of sufficient length to prevent their discovery by manual or automated systematic attack or pure guesswork. Passwords that are not of sufficient length could result in unauthorized access.

d. CJDC had not implemented procedures to have terminals automatically log off after repeated attempts to gain access or when left unattended for a specific period of time. Department of Management and Budget (DMB) Administrative Guide procedure 1310.02 requires that terminals automatically log-off under these conditions. The lack of automatic terminal log-off procedures could result in unauthorized access.

e. CJDC assigned security officer responsibilities to a person who was not in an independent position. Also, CJDC had not established procedures to have the security officer monitor privileged user and other sensitive activities. Privileged users are provided greater capabilities than other users. Assigning security officer responsibilities to a person in an independent position would help ensure the proper performance of security duties. Security officer duties include establishing a security program, enforcing security policies and procedures, monitoring system-recorded security activities and violations, and monitoring privileged user activities. CJDC assigned security officer responsibilities to the technical services manager who had other responsibilities, such as maintaining systems and data bases, that were incompatible with those of the security officer.

In our prior audit, we recommended that CJDC assign its security officer responsibilities to a person who is in an independent position. CJDC responded that it agreed with our recommendation and would pursue, subject to staffing authorizations, the assignment of a security officer who was in an independent position. However, CJDC had not complied with our recommendation.

RECOMMENDATIONS

WE AGAIN RECOMMEND THAT CJDC IMPROVE SYSTEM ACCESS CONTROLS.

WE ALSO AGAIN RECOMMEND THAT CJDC ASSIGN ITS SECURITY OFFICER RESPONSIBILITIES TO A PERSON WHO IS IN AN INDEPENDENT POSITION.

We further recommend that CJDC establish procedures to have the security officer monitor privileged user and other sensitive activities.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with these recommendations and informed us that it will review its system access controls and security administration. CJDC also informed us that this will fall within the responsibilities of a full time security officer position to be established and filled by February 1, 1998.

FINDING

6. Separation of Duties

CJDC had not implemented a proper separation of duties. We noted that Technical Services Section personnel performed on-line application development and maintenance.

The specialized knowledge of the Technical Services Section personnel and their assigned duties create an opportunity for these personnel to bypass system controls, circumvent error messages, and enter unauthorized transactions. As such, they should not be assigned responsibilities for application development and maintenance.

Clearly defining and separating the functions of technical services and application development and maintenance to eliminate the performance of incompatible functions would help ensure proper controls over application development, system software maintenance, and data integrity.

In our prior report, we recommended that CJDC implement a proper separation of duties. CJDC responded that it believed that civil service class descriptions

allowed for the programming of complex systems by Technical Services Section programmers. CJDC also responded that the issue of separation of duties was met because the systems were administered by the LEIN Field Services Section, which controlled the areas of development and security. However, sound internal controls dictate that Technical Services Section personnel should not perform on-line application development and maintenance because of their ability to bypass established controls.

RECOMMENDATION

WE AGAIN RECOMMEND THAT CJDC IMPLEMENT A PROPER SEPARATION OF DUTIES.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with the recommendation. However, CJDC informed us that it now has in place a single section which retains the responsibilities previously divided across the CJDC Technical Services and Applications Development Sections. CJDC informed us that it will address the issue of separation of duties within the new section by creating a new position with responsibilities limited to maintaining system software.

FINDING

7. Network Security

MSP had not developed complete control procedures for network security. Our review of controls over network security disclosed:

a. MSP had not established a network administrator position. Network administrator duties include establishing and maintaining network security, organizing and configuring network resources, and establishing a systematic data backup and retrieval process.

   A network administrator position would help ensure the security and effective management of MSP's network. MSP had 65 local area network* (LAN) sites

* *See glossary on page 33 for definition.*

throughout the State, which collectively could be viewed as one network. MSP staff used the LANs to access law enforcement applications, share files, and transmit electronic mail.

MSP delegated network administrator responsibilities to various CJDC personnel because of staff shortages. However, these personnel were unable to effectively carry out assigned network administrator functions.

b. MSP did not require the monitoring of firewall* logs. Firewalls are used to control which users, services, and information can enter or exit a network. MSP should monitor firewall logs to help identify improper attempts to access its networks. Monitoring firewall logs could also help MSP identify potential problems with firewall configurations by becoming aware of services or users not known to have system access.

c. MSP did not require network users to periodically change their passwords. DMB Administrative Guide procedure 1310.02 requires that passwords be periodically changed. The frequency of password changes should be based on the importance of the system or data being accessed.

Periodically changing passwords could help prevent unauthorized access to confidential and sensitive information contained on LANs.

RECOMMENDATION

We recommend that MSP develop complete control procedures for network security.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendation and informed us that this area will be addressed by the new security officer.

** See glossary on page 33 for definition.*

FINDING

8. Disaster Recovery and File Backup

CJDC did not fully plan for recovery from a disaster and secure backup files. We noted the following weaknesses:

a. CJDC and its users did not complete and test a written disaster recovery plan. Such a plan includes procedures for recovery from a disaster, such as fire, tornado, or sabotage, and identifies the materials, personnel, equipment, and communication systems necessary to process critical systems at another facility.

b. CJDC did not fully document procedures for tape file backup, retention, and storage. Clear and complete procedures are necessary to help ensure that tapes can be effectively and efficiently controlled. We noted that the tape librarian sent critical tapes off site based on undocumented schedules. We also noted that CJDC was unable to fully recover lost data because of problems with backup tapes when one of its servers* became disabled. Periodic testing of the backup and recovery procedures could have identified these problems prior to the loss of the data.

c. CJDC stored some backup tapes in an unlocked vault in the computer room. CJDC did not restrict access to this tape location.

d. CJDC did not identify and store critical documentation at an off-site location. Identifying and storing critical documentation off site would help ensure the safety of documentation in case a disaster occurs at the main processing site.

e. CJDC did not have an alternative power source to protect against power outages.

   Although infrequent, CJDC operations cease when power outages occur. One such outage resulted in the loss of access to law enforcement information systems for approximately seven hours.

** See glossary on page 33 for definition.*

In our prior audit, we recommended that CJDC fully plan for recovery from a disaster and secure backup files. CJDC agreed with our recommendations but had not complied with them.

RECOMMENDATIONS

WE AGAIN RECOMMEND THAT CJDC FULLY PLAN FOR RECOVERY FROM A DISASTER AND SECURE BACKUP FILES BY:

(a) COMPLETING AND TESTING A WRITTEN DISASTER RECOVERY PLAN.

(b) FULLY DOCUMENTING PROCEDURES FOR TAPE FILE BACKUP, RETENTION, AND STORAGE.

(c) LOCKING THE COMPUTER ROOM VAULT AND RESTRICTING ACCESS TO IT.

(d) IDENTIFYING AND STORING CRITICAL DOCUMENTATION AT A SECURE OFF-SITE LOCATION.

(e) OBTAINING AN ALTERNATIVE POWER SOURCE.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendations and informed us that these items will be discussed as part of the migration to the Michigan Information Processing Center or another platform. MSP also informed us that an alternative power source is now being put in place and that a completed disaster recovery plan will be put in place by July 1, 1999.

FINDING

9. Computer Room Access

CJDC did not restrict and effectively monitor access to the computer room. Our review of computer room access disclosed the following weaknesses:

a. CJDC did not restrict access to the computer room. CJDC authorized over 50 nonoperations personnel access to the computer room. This included vendor personnel and Technical Services Section personnel with specialized knowledge

that would enable them to bypass established system controls. CJDC also authorized computer room access to other personnel who had no need for access, such as application systems development and secretarial staff.

In addition, CJDC did not properly configure its voice access control system. As a result, operations staff provided inappropriate access to some individuals. Also, CJDC did not effectively use available options to restrict access to certain computer room doors. Further, operations staff routinely ignored the access point monitor that noted the status of various computer room doors because it registered false alarms.

Effectively restricting access to the computer room and having operations personnel accompany and oversee all other personnel granted access would help prevent unauthorized use of the computer system and interference with computer operations.

In our prior report, we recommended that CJDC restrict access to the computer room. CJDC agreed with our recommendation but had not complied with it.

b. CJDC did not provide video recording capabilities for monitors set up in the computer room to view critical areas. CJDC should equip monitors with video recording capabilities to help provide a record of computer room activities.

c. CJDC did not update the computer operations procedure used to inform operations staff of personnel who require after-hours access. CJDC should update these procedures to help prevent unauthorized individuals from gaining computer room access.

RECOMMENDATIONS

WE AGAIN RECOMMEND THAT CJDC RESTRICT ACCESS TO THE COMPUTER ROOM TO OPERATIONS PERSONNEL.

We also recommend that CJDC effectively monitor access to the computer room by:

(a) Providing video recording capabilities for monitors.

(b) Updating the computer operations procedure used to inform operations staff of personnel who require after-hours access.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with the recommendations and informed us that unrestricted access will not be allowed to any non-MSP employees. In addition, CJDC informed us that a list of all employees needing access will be constructed.

FINDING

10. User Identification Codes and Station Controls

CJDC did not have sufficient internal controls over user identification codes and stations. We noted the following weaknesses:

a. CJDC did not provide unique user identification codes for system software files. Technical Services Section personnel used the same usercode to access system software files. This made it impossible to identify which user performed each activity.

   Providing individual user identification codes for each user would help ensure accountability for system changes.

b. CJDC provided many user terminals with unnecessary system user, privileged user, and control station capabilities. These capabilities enable users to perform sensitive functions and could result in unauthorized access and changes to software or data.

   Removing unnecessary capabilities would help reduce the risk of unauthorized access and changes.

c. CJDC maintained excess user stations on its system. We reviewed 26 user stations and noted 11 disabled stations that either had never been used or had become obsolete. Maintaining excess user stations results in reduced control in overall station security.

In our prior audit, we reported these conditions and CJDC responded that it would comply with the corresponding recommendations. However, it had not done so.

RECOMMENDATIONS

WE AGAIN RECOMMEND THAT CJDC:

(a) PROVIDE UNIQUE USER IDENTIFICATION CODES FOR SYSTEM SOFTWARE FILES.

(b) REMOVE UNNECESSARY SYSTEM USER, PRIVILEGED USER, AND CONTROL STATION CAPABILITIES.

(c) REMOVE UNUSED OR OBSOLETE USER STATIONS.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendations and informed us that the new security officer and dedicated technical services position will work together to develop a plan.

FINDING

11. Production Disk Pack Controls

CJDC did not have sufficient internal controls over the use of its production disk pack. The production disk pack contains the computer programs used to process data. Our review disclosed:

a. Both programmers and systems analysts had access to the programs stored on the production disk pack. Specifically, each:

(1) Accessed and copied programs without management approval.

(2) Did not use usercoding to restrict program access to specific users.

(3) Created the program production object code file, which is used to process actual data, without management approval.

(4) Copied modified program source code and test object code to the production disk pack without management approval.

Controlling access to programs stored on the production disk pack would help reduce the risk of unauthorized program changes.

b. CJDC staff did not always obtain supervisor approval on application program revision requests (APRRs) or service request numbers before placing programs into production. Our review disclosed 35 (9.7%) of 360 APRRs without an approving signature or service request number.

The CJDC Policy and Procedures Manual requires that programmers submit an APRR when removing, adding, or changing production programs. A properly completed APRR includes the signature of the programmer's supervisor and the service request number. Having a supervisor formally review and approve programs and including a service request number on APRRs before placing them into production would help ensure the integrity of programs and data.

c. CJDC had not implemented controls to prohibit or detect access to database files by programs in test status. Controlling access of database files by programs in test status would help ensure the integrity of data.

Although we did not note any errors as a result of this weakness, implementing such controls would help ensure the integrity of the data base.

d. CJDC stored obsolete and possibly different versions of programs on the production disk pack. We reviewed 30 of CJDC's 978 production programs and found:

(1) Obsolete production object code files for 3 (10%) production programs.

(2) Different modification dates for the source code and production object code files for 3 (10%) production programs.

Removing obsolete files and reviewing source code and production object code creation dates would help ensure the use of the correct version of programs to process user data.

In our prior audit report, we recommended that CJDC strengthen control over the use of its production disk pack. CJDC agreed with our recommendation but had not complied with it.

RECOMMENDATION

WE AGAIN RECOMMEND THAT CJDC STRENGTHEN CONTROL OVER THE USE OF ITS PRODUCTION DISK PACK.

AGENCY PRELIMINARY RESPONSE

MSP agreed with the recommendation and informed us that it will review the use of the production disk pack. In addition, MSP informed us that the new technical services position will investigate and place into production identified security software. MSP also informed us that controls requiring signatures on APRRs will be strengthened, and a software librarian position will be requested by April 1, 1998 to provide control of the production disk packs.

FINDING

12. Database Security

CJDC had not developed control procedures to ensure the complete security of database files. Our review disclosed the following weaknesses:

a. CJDC had not developed control procedures to limit access to database guard files. Guard files help restrict access to data bases that contain sensitive or confidential information. As such, access to the guard files should be limited to help ensure accountability and integrity of the data bases.

We noted that 9 Technical Services Section staff had the ability to add and delete users from guard files. In addition, CJDC could not ensure the

accountability of changes to guard files because CJDC used group user codes to control access to guard files. CJDC informed us that Technical Services Section staff needed access to guard files during emergencies. However, we question the need for 9 Technical Services Section staff having continuous guard file access capabilities. We noted that only 2 of the Technical Services Section staff actually made changes to guard files.

b. CJDC used a utility software package to correct database errors but did not develop control procedures to maintain an audit trail documenting its use. A log documenting use of the utility software would provide an audit trail to help monitor it and ensure appropriate changes to data bases.

RECOMMENDATION

We recommend that CJDC develop control procedures to ensure the complete security of database files.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with the recommendation and informed us that it will review database control and security procedures. CJDC also informed us that the new security officer, working with the technical services position, will be given responsibility to ensure that guard file access is limited to proper staff. In addition, CJDC informed us that the use of the utility software package to correct database errors will be eliminated.

FINDING

13. Documentation Standards

CJDC had not established comprehensive system documentation standards as specified in DMB Administrative Guide procedure 1310.07.

We noted that CJDC did not prepare complete system documentation. For example, CJDC documentation lacked such items as system overviews, detail design specifications, and system test plans and results. DMB Administrative Guide procedure 1310.07 requires documentation standards to include such items.

The establishment of complete documentation standards would help CJDC ensure that systems are consistently and sufficiently documented and efficiently maintained.

In our prior report, we recommended that CJDC establish comprehensive documentation standards. CJDC agreed with our recommendation but had not complied with it.

RECOMMENDATION

WE AGAIN RECOMMEND THAT CJDC ESTABLISH COMPREHENSIVE SYSTEM DOCUMENTATION STANDARDS.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with the recommendation and informed us that it will move toward a comprehensive system documentation plan as required by DMB Administrative Guide procedure 1310.07. CJDC also informed us that a technical writer position will be obtained by October 1, 1998 with responsibility to ensure compliance with this standard.

FINDING

14. Tape Control Procedures

CJDC had not established and implemented complete tape control procedures. We noted the following weaknesses:

a. CJDC did not regularly perform a documented inventory of the tape library. Proper controls require that a periodic inventory of the tape files be performed and documented to ensure the accuracy of the tape records.

b. CJDC did not require tapes to be wiped clean before reuse. Tapes may contain confidential information that could be obtained by unauthorized individuals. Requiring tapes to be wiped clean before reuse would help prevent the unauthorized release of confidential information.

RECOMMENDATION

We recommend that CJDC establish and implement complete tape control procedures.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with the recommendation and informed us that it will establish and implement inventory control procedures within the tape library system by October 1, 1998. CJDC also informed us that the issue of wiping tapes clean before reuse will be investigated by April 1, 1998 and a resolution will be put in place by July 1, 1998.

FINDING

15. Output Distribution

CJDC had not developed complete control procedures for the distribution of output.

Our review disclosed that CJDC did not ensure the labeling of confidential reports as confidential. Also, CJDC did not require users to sign for confidential output before releasing it to them.

DMB Administrative Guide procedure 1310.02 requires that applicable reports be labeled as confidential. The procedure also requires that authorized signatures be obtained before the release of confidential information.

Developing control procedures for the distribution of output would help CJDC prevent the improper distribution of confidential output.

RECOMMENDATION

We recommend that CJDC develop complete control procedures for the distribution of output.

AGENCY PRELIMINARY RESPONSE

CJDC agreed with the recommendation and informed us that the new security officer will establish distribution standards for output documents by July 1, 1998.

Glossary of Acronyms and Terms

APRR	application program revision request.
authentication	A process to identify users and access rights to a system.
CANDE	Command and Edit (system software program).
CJDC	Criminal Justice Data Center.
confidence level	A percentage that expresses the probability that the actual error in the population is contained within the range of an estimate.
DMB	Department of Management and Budget.
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.
entering agencies	Law enforcement agencies that input information into LEIN.
FBI	Federal Bureau of Investigation.
firewall	Used to separate internal networks from external networks. A means of controlling which users, services, and information can enter or exit a network.
Law Enforcement Information Network (LEIN)	The Michigan law enforcement computer system and the series of computer terminal locations which allow criminal justice agencies to enter, and have access to, data.

LEIN Policy Council	The council created to provide for the establishment of policy and the promulgation of rules governing the use of LEIN.
local area network (LAN)	A data network intended to serve a small area.
MSP	Michigan Department of State Police.
National Crime Information Center (NCIC)	The computer system at the Federal Bureau of Investigation's national headquarters, which provides out-of-state criminal justice information files to all local, state, and federal agencies. Through NCIC, LEIN users are able to receive out-of-state criminal justice information files.
National Law Enforcement Telecommunications System (NLETS)	The message switching computer link between Michigan LEIN users and other states. Through NLETS, LEIN users are able to communicate with out-of-state criminal justice agencies and to access motor vehicle and driver record files.
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.
precision	A measure of the closeness of a sampling estimate to the corresponding population characteristic at a specific sampling risk.
reportable condition	A matter coming to the auditor's attention that, in his/her 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.

server	Computers that share their resources, such as printers and files, with other computers on a network.
terminal agency	A criminal justice agency in which a LEIN terminal is physically located or an agency that has access to LEIN through a terminal connected to an authorized satellite computer.