Legislative Audit Division

State of Montana

Report to the Legislature

November 2004

Information System Audit

Criminal Justice Information Network (CJIN)

Department of Justice

This report contains the results of an information system audit of the Department of Justice CJIN operation. The report contains four recommendations to strengthen CJIN security.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

04DP-08

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Several staff hold certifications in information industry practices and auditing. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator John Cobb	Representative Dee Brown
Senator Mike Cooney	Representative Tim Callahan
Senator Jim Elliott, Vice Chair	Representative Hal Jacobson
Senator John Esp	Representative John Musgrove
Senator Dan Harrington	Representative Jeff Pattison, Chair
Senator Corey Stapleton	Representative Rick Ripley

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

November 2004

The Legislative Audit Committee
of the Montana State Legislature:

The Legislative Audit Division Information Systems auditors conducted an audit of the Montana Department of Justice Criminal Justice Information Network. The audit was limited to the review of Department of Justice compliance with state statutes requiring system security. This report contains four recommendations addressing Department of Justice security controls operation. Department of Justice management's response to these recommendations is located at the end of the report.

Respectfully submitted,

(Signature on File)

Scott A. Seacat
Legislative Auditor

Room 160, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@state.mt.us

Legislative Audit Division

Information System Audit

Criminal Justice Information Network (CJIN)

Department of Justice

Members of the audit staff involved in this audit were George R. Brown, Charles Nemec, and Dale Stout.

Table of Contents

Elected, Appointed and Administrative Officials

Department of Justice

Mike McGrath, Attorney General
Larry Fasbender, Deputy Director/Chief of Staff

Information Technology Services Division
Steve Tesinsky, Administrator

Criminal Justice Information Service Bureau
Nancy Bloom, Acting Bureau Chief

Chapter 1 - Introduction and Background

Introduction and Background

The Montana Legislature authorized a permanent law enforcement communications system and mandated the Montana Attorney General, who is also Director of the Montana Department of Justice (Justice), to establish and operate the system. The Montana Department of Justice built the Criminal Justice Information Network (CJIN) for this purpose. The Attorney General is vested with the authority to administer all operational phases of CJIN and Department of Justice staff are responsible for CJIN's daily operation.

CJIN is available to law enforcement agencies designated in statute, established by the governor's executive order, or approved by the Montana Attorney General.

We audited CJIN due to its importance as a primary public safety communications system. CJIN connects local agencies to state criminal history files, state vehicle and driver's license files, and priority or "hot" files. CJIN connects Montana to national agencies such as the Federal Bureau of Investigation (FBI) and out-of-state resources such as the National Law Enforcement Telecommunications System and the National Crime Information Center (NCIC). CJIN is not only a record exchange system but also an identification tool providing real-time information to law enforcement officers operating in the field. CJIN is visible to the public as the tool law enforcement officers use in the field to identify people and vehicles. For example, a law enforcement officer accesses CJIN via radio or mobile data terminal when making a traffic stop.

Currently, there are approximately 130 Montana law enforcement agencies using CJIN.

Reasonable Precautions

The legislature established CJIN as a permanent law enforcement telecommunications system in 1967 and later updated statutes governing CJIN with the "Montana Criminal Justice Information Act of 1979."

Chapter 1 - Introduction and Background

The 1979 legislature recognized system security by mandating law enforcement agencies protect criminal justice information systems under their control. Statutes require agencies take reasonable precautions and establish procedures to protect the system and data from damage, to prevent damage from hazards and to recover from hazards.

Compliance Requirements

State law and written agreement with the U.S. Department of Justice designate the Montana Department of Justice as the agency responsible for CJIN. Montana Department of Justice directly operates the "core" CJIN network, which holds Montana data and is the entry point for interacting with agencies outside of the state. The "core" end of the network is located in Helena.

Each local law enforcement agency is responsible for data, staff and equipment security and operation at its end of the network. This responsibility is established in a written agreement between the Attorney General and the local agency.

For this audit, we reviewed CJIN operations to determine if the Montana Department of Justice is meeting statutory intent by taking reasonable precautions to protect CJIN from hazards.

We identified state laws applicable to CJIN and determined that security related statutes are the important CJIN compliance requirement. Since CJIN is the entry point to Montana residents' driver's licenses, vehicle records, and criminal file information, CJIN security controls the access to this information. Security is also important because CJIN must be available to law enforcement officers for immediate use and protecting CJIN equipment is essential to maintaining availability.

Department of Justice personnel operate CJIN to comply with state statutory requirements. These key requirements are summarized as follows:

- Security: Only people authorized by the Montana Department of Justice can physically access CJIN equipment and only authorized people can view the data;
- Security: CJIN core network hardware and software are protected from malicious or accidental events so that CJIN network remains in service and information is available to law enforcement officers.

Audit Objective, Scope, and Methodology

Our objectives:

- Identify the state security requirements applicable to CJIN and
- Determine how well the Department of Justice is operating CJIN in meeting these requirements

By law, the Department of Justice has a duty to safeguard its information and implement safeguards to deal with and recover from threats to its information (2-15-114, Montana Code Annotated (MCA), Security responsibilities of departments for data). Justice also has a duty to protect the security of any criminal justice information system under its control by taking reasonable precautions and establishing procedures to protect the system and the information stored in the system from damage and for the prevention of and recovery from hazards such as fire, flood, power failure, and entry into secure areas by unauthorized persons (44-5-401, MCA, Criminal justice information system security).

To determine whether Justice is meeting security requirements, we requested Department of Justice security and contingency (emergency) plans, observed CJIN operations, interviewed staff, and tested CJIN equipment. We then obtained and reviewed information security policy and guidance released by the National Institute of Standards and Technology, software and hardware vendors for the products used in CJIN, Information Systems Audit and Control Association – Control Objectives for Information and Related Technology, and the Federal Bureau of Investigation.

We reviewed the Department of Justice CJIN environment and identified risks to CJIN security. We determined the corresponding

safeguards that reduce these risks. These safeguards were examined to confirm their existence and operation.

- CJIN firewall operation and maintenance ensure the firewall is effectively preventing unknown or unauthorized computers from accessing the network.
- Software updates to CJIN computers reduce the opportunity for other computers or programs to interfere with CJIN computers' ability to exchange information.
- Department of Justice CJIN Help Desk personnel are knowledgeable and available to local law enforcement agencies to assist in mitigating network technical problems.

The audit was conducted in accordance with Government Auditing Standards published by the U.S. Government Accountability Office.

Results

We are making four recommendations to Department of Justice management to better operate CJIN. Two recommendations improve the effectiveness of CJIN safeguards by advising Justice staff to monitor how the firewall and software updates are operating. Two recommendations improve Justice staff's ability to operate CJIN by using security and contingency planning.

Chapter 2 - CJIN Security

The legislature recognized the importance of CJIN security by mandating law enforcement agencies to protect any criminal justice information systems under their control. The law instructs agencies to take reasonable precautions by establishing procedures to protect and recover from hazards. The following audit recommendations are the results of our work and are intended to assist the Department of Justice in meeting statutory requirements.

Firewall Operation

Issue: No CJIN firewall monitoring procedures are in place to ensure the firewall is effectively protecting CJIN.

Firewall Operation and Its Importance

Department of Justice personnel have implemented CJIN core network security by placing the network equipment behind a "firewall." The firewall is the first line of defense between outside computers and CJIN network equipment. The firewall protects the core network by examining a computer's address when the computer requests access to CJIN. If the firewall recognizes the address, then the network request is granted, otherwise the request is dropped and the outside computer is denied access. The key to operating the firewall as an effective safeguard is ensuring the address list the firewall refers to is current and only contains computer addresses granted and approved by CJIN management.

We evaluated firewall operation by examining the firewall's list of allowed addresses and comparing it to current and authorized law enforcement agency computer addresses. We determined that 93 of approximately 400 addresses were either outdated, duplicate addresses, or unnecessary and should be removed from firewall access. Other Justice safeguards prevented unauthorized CJIN connections from launching through these addresses.

We discussed firewall operation with Justice staff and learned they do not have firewall-monitoring guidance. There are no scheduled staff assignments or monitoring instructions providing Justice staff with a clear understanding of who performs monitoring and how it is best carried out.

Effective safeguard operation requires descriptions on how the safeguard should operate, be checked and how often the specified person should perform the task. For example, one firewall monitoring method is assigning an individual to periodically compare firewall addresses with authorized addresses. Such a procedure would identify oversights, such as the 93 addresses, so staff could correct them before firewall operation is impacted. Without timely and scheduled monitoring, the firewall may not be effective, creating a security risk instead of a safeguard.

Recommendation #1
We recommend the Department of Justice management monitor the firewall to ensure the firewall is effectively operating and safeguarding CJIN.

Software Updates

Issue: No software update monitoring procedures are in place for ensuring current software updates are installed and effectively protecting all CJIN computers.

Software Updates and Their Importance

Networks are inherently vulnerable to outside interference. Department of Justice management recognizes this weakness and the need to protect CJIN computers from security problems that interfere with CJIN's communication and information exchange mission. Justice staff use software updates as an important safeguard to protect CJIN computers for this purpose.

Software updates are vendor created changes to its product (computer code), fixing vulnerabilities or adding security features. Updates can prevent unauthorized people or programs from using a computer without the owner's permission and, sometimes, knowledge. For CJIN, updates are effective in reducing the opportunity for outside interference. However, the updates have to be installed for the computer to be resistant to interference.

Justice personnel are not monitoring update installation for all CJIN computers. Since Justice is responsible for CJIN security, monitoring whether updates are successfully installed or not is critical to keeping CJIN computers available and exchanging information. Updating all computers is especially important since even one unprotected computer means the network is vulnerable.

We evaluated how Justice staff managed update installation by examining the update acquisition and distribution operation and contacting other law enforcement agency staff that receive updates through Department of Justice.

We selected seven law enforcement agency staff responsible for 11 CJIN computer locations to determine update installation status. One person responsible for three locations had overlooked the updates and was not certain when any were last installed. One person was uncertain about how to identify a successful installation. Three people responsible for five locations followed the installation instructions. One person refused to discuss security issues over the phone. One agency did not respond to this inquiry and the person at one agency had retired leaving no one available to answer questions.

Justice staff do not directly monitor update installation on all computers since most computers are owned by other law enforcement agencies. However, CJIN security is dependent on all computers being updated regardless of computer ownership. For that reason, it is necessary to ensure all computers have updates installed for CJIN to be secure.

One way of ensuring computers are updated is through the existing CJIN User Agreement between Justice and local agencies. The agreement could clarify update responsibilities and monitoring options.

For example, the agreement could stipulate:

- Who is responsible for update installation.

- Current updates are a condition of connecting to CJIN.
- Justice will confirm agency update status.

An effective method of ensuring updates are in place strengthens CJIN operations at both the state and local law enforcement agencies.

Recommendation #2
We recommend the Department of Justice management monitor software update installation to ensure all CJIN computers have current updates.

Security Plan

Issue: Department of Justice management has no CJIN security plan.

Security Planning and Its Importance

A common source of information system disruption is security failure. The legislature recognized this potential and enacted two laws on the subject. One statute (MCA 2-15-114) instructs state agency management to develop written policies and procedures to ensure data security, while a second directs a law enforcement agency to protect the security of any law enforcement information system under its control by establishing procedures to protect the system (MCA 44-5-401).

Department of Justice staff were unable to provide a security plan or security operating procedures when we requested this information. The statutory security requirements and the first two report recommendations would be better addressed if the Department of Justice had a security plan. A security plan is the written policy and procedures explaining how Justice management meets security requirements, such as those in Montana law. For example, management uses a plan to describe:

- Information and equipment security risk,
- Acceptable risk policy or procedures creating safeguards that reduce risks,

- Safeguard operating procedures,
- Procedures measuring safeguard effectiveness,
- Alternate procedures if a safeguard fails, and
- Changing policy or procedures when risks and requirements change.

The resulting plan is in writing so the people accountable for security can assign responsibility and provide operation and monitoring details to those who carry out security.

According to Department of Justice management, resource limitations have prevented a security plan from being developed and put into practice. However, with the recent addition of a Security and Disaster Recovery Officer, we believe there is an individual with the appropriate background available to develop and test a plan if directed by management to this task.

Recommendation #3
We recommend Department of Justice management develop, document, and maintain a CJIN security plan.

CJIN Contingency Plan

Issue: Department of Justice management has no CJIN contingency plan.

Contingency Planning and Its Importance

Contingency planning is making sure CJIN continues operating in emergencies, providing law enforcement with communications.

Contingency planning is different from security planning because critical CJIN resources, like power or communications, are outside of Justice's control. Disruptions can come from diverse sources like natural disasters or peoples' malicious acts. No Justice safeguard can prevent these events. However, Justice can minimize the disruption by developing alternatives or replacements when the original resources are damaged or destroyed.

Contingency planning is not a new or unique compliance requirement for the Department of Justice. The Montana Legislature recognized the value of having alternatives to keep CJIN operating when enacting the Montana Criminal Justice Information Act of 1979. The law requires a law enforcement agency to protect the information system under its control taking precautions and establishing procedures for the recovery from hazards (MCA 44-5-401).

The FBI includes a contingency planning requirement in its CJIN agreement with Justice. FBI policy describes a written plan that will:

- Be routinely reviewed and updated;
- Be tested on a regular schedule to ensure operating feasibility;
- Quickly restore vital operations; and
- Minimize downtime.

Justice staff are aware of the need for alternatives and have methods for periodic information backup and for operating communications at an alternate site. However, Justice management could not provide a contingency plan or established procedures for alternative operations when we requested this information.

According to Department of Justice management, resource limitations have prevented such a plan from being developed and practiced. However, with the recent addition of a Security and Disaster Recovery Officer, we believe an individual with the appropriate background is available to develop and test a contingency plan if directed to this task.

Recommendation #4

We recommend the Department of Justice management develop, document, and maintain a CJIN contingency plan.

Department Response

ATTORNEY GENERAL
STATE OF MONTANA

Mike McGrath
Attorney General

Department of Justice
215 North Sanders
PO Box 201401
Helena, MT 59620-1401

November 1, 2004

Mr. Scott Seacat, Legislative Auditor
Legislative Audit Division
Helena, MT 59620

Dear Mr Seacat:

The Montana Department of Justice, Information Technology Services Division has reviewed the audit that was performed on the Criminal Justice Information Network (CJIN). Listed below are the responses to the four findings outlined in the audit.

1) Firewall Operation Finding

Issue: No CJIN firewall monitoring procedures are in place to ensure the firewall is effectively protecting CJIN

Recommendation: We recommend the Department of Justice management monitor the firewall to ensure the firewall is effectively operating and safeguarding CJIN.

Response: We concur with this recommendation. However, it should be noted that the firewall is a first line of defense in a defense in depth strategy. There are several levels of protection within the system. Even if an IP address is given access through the firewall, connectivity to the system requires a valid username and password as well as a system administrator predefined IP address on the server. We currently audit the firewall twice a year, however, due to limitations placed on us by Department of Administration, we have little control of the firewalls themselves. It is our intention to not only audit the firewalls on a more frequent basis but to follow-up on the findings on a more frequent basis.

2) Software Update Finding

Issue: No software update monitoring procedures are in place for ensuring current software updates are installed and effectively protecting all CJIN computers.

Recommendation: We recommend the Department of Justice management monitor software update installation to ensure all CJIN computers have current updates.

Response: We concur with this recommendation. Given Microsoft license agreements, we cannot patch systems we do not own. We were already in the process of developing a Security Addendum that will require the signature of the agency administrator. Where we own the computer, we will give the customer notice of the patches and then install and run them as required. If we do not own the computer, we will require installation of the patches in a timely fashion. Failure to do so could result in the Department of Administration disconnecting access to the state network. The state policies already allow for this and the Department of Justice defers to the Department of Administrations guidelines. We are also in the process of developing information security training that emphasizes to all CJIN users the need for patching systems as well as how to accomplish this task.

TELEPHONE: (406) 444-2026 FAX: (406) 444-3549 E-MAIL: contactdoj@state.mt.us

3) Security Plan Finding

Issue: Department of Justice management has no CJIN security plan.

Recommendation: We recommend Department of Justice management develop, document, and maintain a CJIN security plan.

Response: We concur with this recommendation. We are currently in the process of documenting devices on the network to develop a risk assessment of those devices. Ultimately, this will direct what safeguards are to be put in place. We have also developed procedures and documentation on incident response to better handle and learn from incidents that affect CJIN. This and contingency planning are the top priorities for our new Disaster and Recovery Officer.

4) Contingency Plan Finding

Issue: Department of Justice management has no CJIN contingency plan.

Recommendation: We recommend the Department of Justice management develop, document, and maintain a CJIN contingency plan.

Response: We concur with this recommendation. As stated in the security plan finding, we are currently doing a comprehensive inventory of all devices, software and systems that relate to the operation of CJIN. Part of this inventory includes identifying backup systems, location and procedures for information backup. While there is currently not a written document in place, staff is aware of the procedures and the steps required to reestablish operation. We are aggressively working toward getting these procedures and steps in a documented form.

Very Truly Yours,

MIKE MCGRATH
Attorney General