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

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Dale Stout, Information System Auditor

DATE: February 19, 2006

RE: Follow-up IS Audit:
Criminal Justice Information Network (06SP-023)
Montana Department of Justice (orig. 04DP-08)

INTRODUCTION

We presented our information system (IS) audit of the Montana Department of Justice's Criminal Justice Information System to the Legislative Audit Committee in November 2004. The report contains four recommendations. The recommendations relate to:

- Monitoring the firewall to ensure the firewall is effectively operating and safeguarding CJIN;
- Monitoring software update installation to ensure all CJIN computers have current updates;
- Developing, documenting and maintaining a CJIN security plan; and,
- Developing, documenting and maintaining a CJIN contingency plan.

We requested and received information from the Montana Department of Justice (DoJ) personnel regarding progress toward implementation of our report recommendations. This memorandum summarizes information on the implementation status of each audit recommendation.

BACKGROUND

The Criminal Justice Information Network (CJIN) connects local agencies to state criminal history files, state vehicle and driver's license files, and priority or "hot" files. It also connects Montana to national agencies such as the Federal Bureau of Investigations (FBI) and out-of-state resources such as the National Law Enforcement Telecommunications System and the National Crime Information Center. 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. We identified state laws applicable to CJIN and determined that security related statutes are the important CJIN compliance requirements.

Follow-up Discussion

The following sections summarize the report recommendations, and the department's progress towards implementing the recommendations.

Firewall Operation

The firewall is the first line of defense between CJIN networking equipment and outside computers. 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.

After evaluating the firewall's list of allowed addresses with a list of current and authorized law enforcement agency computer addresses, we determined many addresses were either outdated, duplicates or unnecessary and should have been removed from the firewall's list of addresses. We discussed firewall operation with DoJ staff and learned they did not have firewall-monitoring guidance.

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

Recommendation Status: **Implemented**

DoJ management began a process of regularly evaluating the firewall's list of addresses in August 2005. As a result, outdated, duplicate or unnecessary addresses have been removed from the firewall's list of addresses. Another review of the firewall rules is currently underway and updates to the firewall's list of addresses are scheduled to occur.

Software Updates

Software updates are vendor created changes to its product, fixing vulnerabilities or adding security features. Updates can prevent unauthorized people of 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.

DoJ management recognizes the need to protect CJIN computers from security problems that interfere with CJIN's communication and information exchange mission and, accordingly, Justice staff have incorporated regular software updates as part of CJIN's security. However, Justice personnel were not monitoring update installation for all CJIN computers, leaving several CJIN computers without current vendor software updates.

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

Recommendation Status: **Implemented**

There are two types of CJIN computers: DoJ owned and DoJ CJIN client owned. DoJ has implemented a process where DoJ owned CJIN computers are updated automatically every day without user intervention. The computers will automatically check with a specified DoJ computer containing the most current updates and, if needed, automatically install them. This process is monitored through a reporting system allowing DoJ staff to observe the installation

status of each CJIN computer at any point in time. DoJ represents they have no right to use this method on CJIN client owned systems but monitor the patching levels through a technical section of their CJIN client audits. We did not verify this monitoring was taking place.

Security Plan

The purpose of a security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. This 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 responsibilities. Without a written CJIN security plan, security requirements relating to CJIN could be missed as evidenced by the previous two recommendations.

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

Recommendation Status: **Implemented**

DoJ developed a security plan in December 2005 including objectives such as documenting security policies for DoJ applications, data, communications, networks, and physical assets, including CJIN. There have been three revisions to the original document, including the most recent issued in February 2006.

Contingency Plan

Networks can be disrupted by activity outside an entity's control. These include power losses, natural disasters or malicious activity of people outside that entity. A contingency plan addresses these types of disruptions and can minimize their impact by documenting alternative actions to be performed if original resources are damaged or destroyed. DoJ staff recognizes the need for these alternative actions 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.

> Recommendation #4
> We recommend the Department of Justice management develop, document, and maintain a CJIN contingency plan.

Recommendation Status: **Implemented**

Justice management issued their initial CJIN contingency plan in September 2005. Two subsequent revisions have occurred, the most recent in February 2006. In the plan, Justice recognizes the criticality of CJIN's continued operation in the case of a network disruption and lists alternative actions to be performed.