Audit Report

Judiciary
Judicial Information Systems

November 2008

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.
- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

November 18, 2008

Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Judicial Information Systems (JIS) of the Judiciary. Our audit included an internal control review of the JIS data center and the network administered by JIS that supports the Judiciary and Courts of Maryland.

Our audit disclosed that proper internal control had not been established over several significant areas. For example, JIS lacked assurance that critical production data files, security files, and operating systems were adequately protected. In addition, monitoring and control of network traffic was not adequate.

An Executive Summary of our findings can be found on page 5. The Judiciary's response, on behalf of JIS, to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by JIS.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

* **Denotes item repeated in full or part from preceding audit report**

Executive Summary

Legislative Audit Report on
Judicial Information Systems (JIS) of the Judiciary
November 2008

- **Mainframe security controls could be bypassed because certain files, libraries, and programs with special system privileges were not properly controlled, and supervisory personnel did not review and approve all modifications of key system files.**

  Modification access to critical privileged operating system files should be limited to individuals who require such access and unnecessary library and program names with special privileges should be removed. Furthermore, JIS management should conduct and document reviews of all changes to critical operating system files.

- **Modification access to certain critical security software files was not properly restricted or recorded, and numerous employee user accounts could use three system-oriented accounts; these accounts allowed these users unnecessary and unrecorded modification access to data and system files.**

  Modification access to critical security software files should be logged and should be limited to personnel whose job duties require such access, and JIS should discontinue use of these system-oriented accounts.

- **Program change controls and access controls over critical production programs were not adequate.**

  JIS should ensure that only management authorized and properly tested computer programs are placed into production. In addition, direct modification access to critical programs should be limited to users who require such access.

- **A critical network device was not configured securely and numerous vulnerabilities were detected on several web servers.**

  This device should be configured securely and the reported vulnerabilities should be independently verified and remediated where appropriate.

Background Information

Agency Responsibilities and Description

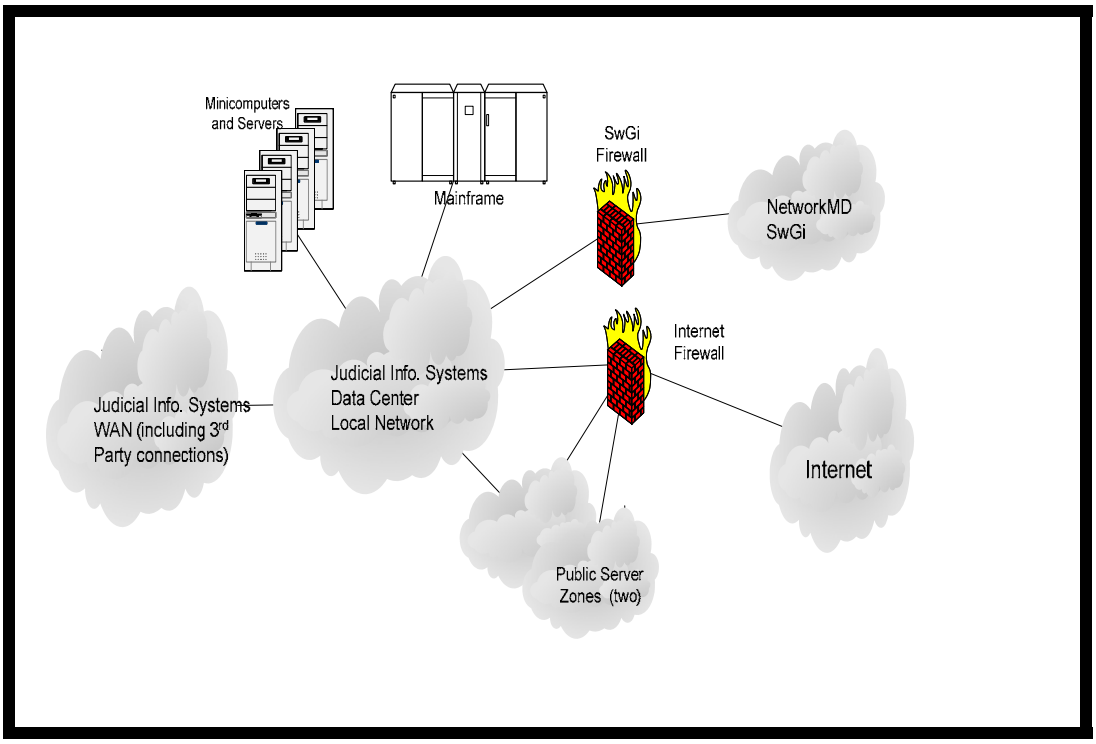
The Judiciary operates the Judicial Information Systems (JIS) on behalf of the State court systems. JIS develops and maintains State court system applications, operates a statewide computer network, and is responsible for data center disaster recovery capabilities. Traffic case dispositions and court case data processed by JIS are supplied to computer systems maintained by the Motor Vehicle Administration and the Department of Public Safety and Correctional Services, respectively. According to the State's records, the JIS fiscal year 2008 operating budget totaled approximately $37.2 million.

JIS operates a mainframe computer for court applications (such as, district court case management) and a server that supports the Maryland Automated Traffic System (traffic citations). In addition, there are eight servers which support the Uniform Court System (UCS). JIS serves three groups of users: public customers, Judicial Data Center personnel, and remote Court users.

JIS also operates a Wide Area Network (WAN) which connects users to the various component units of the Judiciary, including the Administrative Office of the Courts, the District Courts, the Circuit Courts, and the Court Commissioners' offices. The WAN is used to connect the remote court locations to the UCS, which provides court case management to 22 Circuit Courts. The UCS supports case initiation, scheduling, disposition, expungement, and other record keeping. JIS staff connect across the WAN and maintain the regional UCS servers and update the application software. Additionally, the WAN transmits communications from remote court offices to the JIS mainframe applications. Furthermore, 75 local area networks, across all remote court locations, can access the UCS and access external agencies through the Internet. Internet transmissions are controlled by the JIS Internet firewall.

A graphic depiction of JIS and its components appears on the next page.

Overview of the JIS Networking Environment



JIS operates a network that includes numerous servers, minicomputers, a mainframe computer, and connectivity to the Internet and, through its Wide Area Network (WAN), to various Judicial Branch agencies (for example, the District Courts and the Circuit Courts).

Status of Findings From Preceding Audit Report

We reviewed the status of the 11 findings included in our preceding audit report dated February 10, 2005. We determined that JIS satisfactorily addressed seven of these findings. The remaining four findings are repeated in this report.

Findings and Recommendations

Data Center Information System Security and Control

Background

Accepted security principles require organizations to ensure that the information they maintain is accessed by the appropriate persons and for authorized use only. To accomplish this, the Judicial Information Systems' (JIS) computer systems contain security software that is capable of restricting access to system, security, and data files; online transactions; and programs. The related software can also provide a record of all file, transaction, and program modification accesses, and all unauthorized attempted accesses to the computer system. For example, individuals are allowed by the security systems to sign onto various computer processing applications to update critical data files. Unauthorized requests are denied access by the security software. Furthermore, the JIS computer network devices can be configured to provide network security for network users.

Finding 1
Mainframe system security could be bypassed because necessary controls did not exist over critical segments of the operating system software.

Analysis

Controls over certain critical segments of the mainframe operating system software were inadequate, allowing normal security controls to be bypassed:

- All changes to critical operating system files were not subject to review and approval by supervisory personnel. JIS personnel advised us they reviewed changes to critical operating system files on a periodic basis using an automated tool to facilitate monitoring. However, these periodic reviews did not include all changes made to critical system files. This condition could ultimately result in unauthorized or erroneous changes to mainframe data files (for example, court case records). A similar condition has been commented upon in our five preceding audit reports dating back to 1992.

- Access rules over numerous operating system files with special operating system privileges were inadequate. Specifically, improper modifications could be made to many of these files by numerous system users without detection by management. A similar condition was commented upon in our preceding audit report.

- Various library names and program names were defined to the system with special privileges capable of bypassing security controls, but the associated libraries and programs either did not exist or were unnecessary. As a result, libraries or programs using these names could be created that would not be subject to normal security system controls. A similar condition was commented upon in our two preceding audit reports.

Recommendation 1
We again recommend that JIS management conduct and document reviews of all changes to critical operating system files. We also again recommend that JIS restrict modification access to critical, privileged operating system files to individuals who require such modification access, and that such modification accesses be recorded, reviewed, and investigated. Furthermore, we recommend that the results of these reviews and investigations be documented as necessary. Finally, we again recommend that JIS eliminate unnecessary library and program names that could be used to bypass normal security system controls.

Finding 2
Access and recordation controls over critical files were inadequate.

Analysis
Access and recordation controls over critical security software and system files were inadequate. Specifically, we noted the following conditions:

- JIS did not restrict or record modification access to certain critical security software libraries and files. As previously mentioned, JIS uses security software to provide access controls for files, transactions, and other computer resources. However, numerous users had unlogged modification access to several critical security software libraries and files and, for most of these users, such access was unnecessary. As a result, these users could make unauthorized changes to the security software that could alter or impact security controls without detection by management.

- Inadequate access and recordation controls existed for three system-oriented accounts that 38 JIS employee user accounts could use. JIS used a feature of the security software which allows an individual user account to operate under the identity of another account (hereafter called an assumed account) to gain greater access privileges for system operations purposes. However, activity performed under the three assumed accounts was not logged, leaving no accountability of processing performed by any individuals using the assumed

accounts. Also, use of two of the assumed accounts bypassed the security software's controls which led to access control weaknesses involving the security system and operating system on the mainframe computer. Finally, use of the three assumed accounts led to control weaknesses because the security system's access rules allowed these assumed accounts modification access to any mainframe system file. A similar condition was commented upon in our preceding audit report.

Recommendation 2

We recommend that modification access to critical security software libraries and files be logged and limited to personnel whose job duties require such access. We also again recommend that JIS discontinue use of the assumed accounts.

Finding 3

Access controls and security reporting for management transaction operating system files were not adequate.

Analysis

Access controls and security reporting for management transaction operating system files were not adequate. Specifically, we noted the following conditions:

- Numerous users had necessary but unlogged execution access to six critical management transactions, which are programs designed to modify certain related operating system files. In addition, reports identifying the use of critical management transactions (including five of the six aforementioned transactions) were not generated. As a result, changes made to operating system files via these management transactions could occur without management's knowledge and approval.

- Numerous users had necessary but unlogged direct modification access to management transaction operating system files. As a result, unauthorized changes could be made to these management transaction system files and user agency production data files without detection by management.

Recommendation 3

We recommend that use of critical management transactions be recorded and that reports identifying the use of such transactions be generated and reviewed by appropriate supervisory personnel. We also recommend that

modification access to management transaction operating system files be recorded, reviewed, and investigated, and that the results of these reviews and investigations be documented as necessary.

Finding 4
Program change controls and access controls over critical production programs were not adequate.

Analysis
Program change controls and access controls over critical production programs were not adequate. Specifically, we noted the following conditions:

- Adequate control procedures did not exist to ensure that only management authorized and properly tested computer programs had been placed into production. Specifically, computer programmers could modify programs after the programs had been reviewed and approved by supervisory personnel, effectively bypassing the supervisory review process. In addition, the documentation of program changes reviewed by supervisory personnel was created by the programmers responsible for making the program changes. As a result, programmers could make program changes subsequent to the creation of this documentation, which would not be reflected in the documentation. Finally, a comparison of programs actually moved to production to approved program changes was not performed. As a result, there was a lack of assurance that only management authorized and properly tested computer programs have been placed into production. Deficiencies regarding modification and documentation of programs were commented upon in our two preceding audit reports, and the lack of comparison of programs was noted in our preceding audit report.

- Sixty-seven users had unlogged direct modification access to critical production program libraries and, for 27 of these users, such access was unnecessary. These conditions allowed these users to make unauthorized changes to production programs without detection.

Recommendation 4
We again recommend that JIS establish procedures to ensure that only management authorized and properly tested computer programs are placed into production. We also recommend that direct modification access to critical production program libraries be limited to users who require such access and that all such attempted accesses be logged.

Network Security and Control

Finding 5
Monitoring and control of network traffic was not adequate.

Analysis
Monitoring and control of network traffic, from both external and internal sources, was not adequate. Specifically, we noted the following conditions:

- Intrusion detection systems were not properly used to protect critical portions of the network. Specifically, as of May 2008, the intrusion detection system did not include updates from the system vendor for the latest threats since July 2007. In addition, the placement of the intrusion detection system did not protect critical portions of the internal network from threats originating from the Internet, the Statewide Intranet, and from several neutral network zones within the network. Intrusion detection systems gather and analyze network traffic to identify and block network security breaches and attacks, and alert network administrators of these situations.

- Traffic from a neutral network zone, which contained publicly-accessible servers, could access the entire internal network over all ports. While certain servers in this zone needed access to certain devices (over specific ports) in the internal network, most of the devices in this zone did not need such access.

Recommendation 5
We recommend that JIS update its intrusion detection system for the latest threats. We also recommend that JIS implement intrusion detection systems at appropriate locations for the critical portions of its network. Finally, we recommend that traffic from the neutral network zone to the internal network be restricted to comply with a "least privilege" security strategy permitting only necessary access.

Finding 6
A critical network device was not securely configured, and numerous vulnerabilities were detected on several critical web servers.

Analysis
A critical network device was not securely configured, and numerous vulnerabilities were detected on several critical web servers. Specifically, we noted the following conditions:

- An insecure connection protocol was utilized as the primary method for remote administration of a critical network control device. In addition, this device was configured to allow its predefined network traffic routes to be overridden by those routes specified in the network traffic, thereby limiting the effectiveness of this network control device.

- Adequate security measures did not exist for several important network web servers to protect those servers from external and internal exposures, such as from the Internet. We performed vulnerability scans of several critical web servers, and detected 15 instances of vulnerabilities, which the scanning tool identified as high or medium security vulnerabilities. As a result of these vulnerabilities, these servers were not adequately secured from exposures that could result in the loss of data integrity, the interruption of key services, and the improper use of these servers. A similar condition was commented upon in our preceding audit report.

Recommendation 6

We recommend that JIS securely configure the critical network device. We also again recommend that JIS independently verify the aforementioned reported software vulnerabilities and eliminate confirmed vulnerabilities by performing the necessary fixes.

Audit Scope, Objectives, and Methodology

We have audited the Judicial Information Systems (JIS) operated by the Judiciary. Fieldwork associated with our review of JIS was conducted during the period from July 2007 to December 2007. Additionally, fieldwork associated with our review of the network was conducted during the period from December 2007 to June 2008. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine JIS's internal control over its data center and network and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support the State courts and related agencies of the Judiciary. We also determined the status of the findings contained in our preceding audit report on JIS dated February 10, 2005. JIS's fiscal operations are audited separately. The latest report, which covered JIS's fiscal operations, was issued on June 21, 2007.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of JIS operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

JIS management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect JIS's ability to maintain reliable financial records, operate effectively and efficiently and/or comply with applicable laws, rules, and regulations. Our audit did not disclose any significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to JIS that did not warrant inclusion in this report.

The Judiciary's response, on behalf of JIS, to our findings and recommendations, is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the Judiciary regarding the results of our review of its response.

APPENDIX

ROBERT M. BELL
CHIEF JUDGE
COURT OF APPEALS OF MARYLAND
ROBERT C. MURPHY COURTS OF APPEAL BUILDING
361 ROWE BOULEVARD
ANNAPOLIS, MARYLAND 21401-1699

November 12, 2008

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore Maryland 21401

Dear Mr. Myers:

We have received the Legislative Auditor's Draft Audit Report pertaining to the audit of the Judicial Information Systems (JIS), dated October 2008. The following are our responses to the report's findings and recommendations.

Data Center Information System Security and Control

Finding 1

We concur with the finding and recommendation.

- We have acquired and implemented software that identifies and logs all changes to critical operating system files/libraries and operating system parameters. The resulting report is reviewed, recorded, and archived by JIS management on a daily, weekly, and monthly basis.

- We have corrected the access rules to operating systems files with special operating privileges, permitting only employees authorized to update and apply the logging feature to these resources. The Technical Support Unit is the group owner of RIBM. We currently receive a violation report of all individuals attempting access. Reports which include modifications to access rules are monitored, investigated, and documented on a daily, weekly, and monthly basis.

- We also have eliminated all unnecessary library and program names that could be used to bypass normal security systems controls.

Finding 2

We concur with the finding and recommendation.

- We have corrected the access to all critical security software libraries and files, permitting only authorized employees to update access. We have applied a logging feature to the above resources. The Tech Support Unit is the group owner of the group RIBM and currently receives a violation report of all individuals attempting access. Reports which include modification to the access rules are monitored on a daily, weekly, and monthly basis.

- We also have discontinued the use of assumed accounts from the system.

Finding 3

We concur with the finding and recommendation.

- We have implemented a process where the use of critical management transactions are recorded and reviewed by management on a daily basis.

- We also have implemented a process where modification access to management transactions operating system files are recorded, reviewed and investigated by JIS management. The results of their reviews and investigations will be documented as necessary.

Finding 4

We concur with the finding and recommendation.

We have developed processes and procedures to remediate deficiencies noted in the finding. The new Librarian processes and procedures are as follows:

- We have developed a three-tiered approach to move programs into a production system, which takes the modified/changed module to a segregated Quality Assurance level prior to moving it into production. In taking this approach, JIS has addressed the issue of program change being placed in

production prior to management review. While the module is in the interim QUAL level, the programmer is restricted from making any additional changes. This allows the analyst to perform a review and validation test of the module before it is moved into a production system. It is also at this point that the analyst will verify that the documentation provided by the programmer matches the specifications. If the validation testing is successful, the module is moved into production by the Operations Unit. If unsuccessful, the module is rejected and the Operations Unit moves the module back to the test environment for further work by the programmer. Once this revised module is completed, it is reiterated by the same described process. There is also a post-production comparative review of the module by the analyst and senior manager to ensure the module is performing as expected. This new set of procedures will be implemented by November 30, 2008.

- We have established processes and procedures to ensure that direct modification access to critical production program libraries are limited to users who require such access. Update access has been restricted for critical system files to the Operations Unit. The Operations Unit Manager currently receives a violation report of all individuals attempting access. The subsequent listing documents the appropriate access and logging specifications in blue. The Critical Library Changes report is generated on both a weekly and monthly basis with retention in the Control/D product. The report is transmitted to the appropriate personnel for review who must acknowledge the content and save the file to a shared drive for retention. Comments are inserted and the document is filed electronically for future review. In addition, senior managers are assigned the responsibility to perform a review with their subordinates for compliance and sign-off on the reports. This new set of procedures will be implemented by November 30, 2008.

Network Security and Control

Finding 5

We concur with the finding and recommendation.

- The current JIS intrusion detection system does not have the capacity to monitor the entire network so it was positioned to monitor the most heavily traversed section of the network. We are in the process of procuring additional intrusion detection systems that will have sufficient capacity to monitor and report on the entire network.

- The servers that produce the neutral zone network traffic referred to in the finding will be consolidated and additional firewall rules will be created to implement the recommended “least privilege” security strategy.

We estimate that the work needed to implement this finding will be completed by April 30, 2010.

Finding 6
We concur with the finding and recommendation.

- The critical network device referred to in this finding has been secured as recommended.

- We are in the process of verifying the 15 web server vulnerabilities detected during the audit and will recommend the appropriate corrective action to be taken at the end of the process.

  We estimate that the work needed to implement this recommendation will be completed by August 31, 2009.

We believe we have responded in full to all findings and recommendations in the audit report.

Very truly yours,

Robert M. Bell

Frank Broccolina
State Court Administrator

cc: Faye Gaskin, Deputy Court Administrator
Philip S. Braxton, Executive Director Judicial Information Systems
Robert Bruchalski, Deputy Director Judicial Information Systems
Joseph McHugh, Deputy Director Judicial Information Systems
Ssali S. Luwemba, Director of Internal Audit

AUDIT TEAM

Stephen P. Jersey, CPA, CISA
A. Jerome Sokol, CPA
Information Systems Audit Managers

Richard L. Carter, CISA
R. Brendan Coffey, CPA
Information Systems Senior Auditors

Amanda L. Trythall
Staff Auditor