Audit Report

Judiciary
Judicial Information Systems

February 2012

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

February 28, 2012

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, 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 logging and monitoring controls over certain computer system and database files were not sufficient. Also, critical firewalls and routers were not configured to fully protect the Judiciary's network from untrusted third parties.

The Judiciary's response to this audit, on behalf of JIS, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the audit by JIS.

Respectfully submitted,

Bruce A. Myers

Bruce A. Myers, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Table of Contents

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

Background Information

Agency Responsibilities

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 contingency planning. 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 2011 expenditures totaled approximately $34.8 million.

JIS operates a mainframe computer for court applications (such as, district court case management) and a server that supports the Traffic Processing Center (traffic citations). In addition, there are seven 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 has a Wide Area Network (WAN) which operates on an infrastructure owned and supported by a vendor. This WAN connects users to the various component units of the Judiciary including the Administrative Office of the Courts, the District Courts, and the Circuit Courts. 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 JIS mainframe applications. Furthermore, numerous local area networks, across all remote court locations, can access the UCS and can access external agencies through the Internet. Internet transmissions are controlled by the JIS Internet firewall.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the six findings in our preceding audit report dated November 18, 2008. We determined that the JIS satisfactorily addressed five of these findings, and the remaining finding is repeated in this report.

Findings and Recommendations

Network and Data Center Information Systems Security and Control

Background

The Judicial Information Systems' (JIS) mainframe computer system contains 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.

Finding 1
The JIS computer network was not properly secured.

Analysis

Security measures had not been established to fully protect critical network devices and administrative systems from external and internal threats. Specifically, we noted the following conditions:

- Rules on several firewalls and routers allowed numerous unnecessary connections to portions of the JIS network, placing various network devices at risk. For example, we noted firewall rules that allowed IP addresses assigned to vendors unnecessary access to the entire JIS network through all ports.

- Numerous publicly accessible servers residing in neutral network zones on the JIS network had unnecessary access to the entire JIS internal network over many ports. Therefore, there was additional risk of unauthorized access. Such access should be limited to required internal network devices over select ports.

Access rules for critical network devices should use a "least privilege" security strategy that only grants network access privileges needed to perform assigned tasks.

Recommendation 1

We recommend that JIS configure its firewalls and routers to properly secure its network using a "least privilege" security strategy.

Finding 2
Logging and monitoring controls over critical operating system, security system, and database files were not adequate.

Analysis
Logging and monitoring controls over critical operating system, security system, and database files were not adequate. Specifically, we noted the following conditions:

- Direct modifications to a critical database, the use of key database privileges and statements, and operations issued by a critical database account were not logged. In addition, the logs of other database activity that were created were stored in a location that was accessible to the database administrators, and therefore, were susceptible to database administrator modification.

- Supervisory employees responsible for reviewing and approving modifications to critical mainframe operating system libraries and the security software daily report (which identified changes to user capabilities) could also make changes to these same system libraries and user capabilities.

As a result of these conditions, unauthorized or inappropriate modifications to critical operating system, security system, and database files could be made without detection.

Recommendation 2
We recommend that
a. direct modifications to this database, the use of key database privileges and statements, and operations issued by critical accounts be logged;
b. database logs be stored in a location that is not accessible to the database administrators; and
c. reviews of changes to critical operating system libraries and security system reports be performed by individuals independent of the related processes.

Finding 3
Access controls over critical production programs were not adequate.

Analysis
Approximately 40 users had been assigned unnecessary, direct modification access capabilities to critical production and pre-production program libraries. Furthermore, in some cases, the use of the access capabilities was not logged.

These conditions could allow these users to make unauthorized changes to production programs without detection. A similar condition was commented upon in our preceding audit report.

Recommendation 3

We recommend that direct modification access to critical program libraries be limited to users who require such access and that all such attempted accesses be logged (repeat).

Audit Scope, Objectives, and Methodology

We have audited the Judicial Information Systems (JIS) operated by the Judiciary. Fieldwork associated with our audit of JIS was conducted during the period from April 2011 to September 2011. 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. JIS's fiscal operations are audited separately as part of our audit of the Judiciary. The latest audit report on the Judiciary was issued on August 24, 2010. We also determined the status of the findings contained in our preceding audit report on JIS dated November 18, 2008.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of materiality and risk. The areas addressed by the audit included general controls and security controls over operating systems, the security system, databases, firewalls, and routers. 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 findings related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect JIS's ability to 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 to our findings and recommendations, on behalf of JIS, 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

February 27, 2012

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore, Maryland 21201

Dear Mr. Myers:

We are in receipt of the Legislative Auditor's letter dated February 7, 2012, pertaining to findings from the audit of the Judiciary's Judicial Information System. The following responds to those findings:

Network and Data Center Information Systems Security and Control

Finding 1
The JIS computer network was not properly secured.

Recommendation:

We recommend that JIS configure its firewalls and routers to properly secure its network using a "least privilege" security strategy.

Response:

We have configured and will continue to configure rules on firewalls and routers to employ the "least privilege" security strategy, limiting vendor and public access to only the intended devices over specific ports. Many of the specific unnecessary accesses outlined during the audit were removed during the audit process.

We will design and implement firewall and other filtering mechanisms to manage publicly accessible servers residing in neutral network zones, limiting access to only required internal network devices and servers over specific ports.

Finding 2
Logging and monitoring controls over critical operating system, security system, and database files were not adequate.

Recommendation:

We recommend that:

a. Direct modifications to this database, the use of key database privileges and statements, and operations issued by critical accounts be logged;
b. Database logs be stored in a location that is not accessible to the database administrators; and
c. Reviews of changes to critical operating system libraries and security system reports be performed by individuals independent of the related processes.

Response:

We concur with the finding and recommendation.

a. Logging of direct database modifications, use of key database privileges and statements, and operations by critical accounts for the critical database cited was turned on during the audit process.
b. Database logs will be stored in a location that is not accessible to the database administrators.
c. JIS Senior Managers, independent of the related processes, are performing reviews of changes to critical operating system libraries and security system reports. The reports are archived and retained on a protected file share.

Finding 3
Access controls over critical production programs were not adequate.

Recommendation:

We recommend that direct modification access to critical program libraries be limited to users who require such access and that all such attempted access be logged (repeat).

Response:

We concur with the finding and recommendation.

We have implemented member level security access and reporting mechanisms. Privileges for direct modification access to critical program libraries is now limited to only those users who require such access. A process for logging, reviewing and documenting direct modifications access has been implemented.

We believe this responds in full to the findings noted in the audit report.

Very truly yours,

Robert M. Bell

Robert M. Bell

cc: Frank Broccolina
Faye D. Matthews
Ssali Luwemba
Mark Bittner
Robert Bruchalski

AUDIT TEAM

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

R. Brendan Coffey, CPA
Omar A. Gonzalez, CPA
Information Systems Senior Auditors

Eric Alexander
Michael K. Bliss, CISA
Information Systems Staff Auditors