Audit Report

Department of Public Safety and Correctional Services
Information Technology and Communications Division

January 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

January 6, 2012

Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Department of Public Safety and Correctional Services (DPSCS) – Information Technology and Communications Division (ITCD). Our audit consisted of an internal control review of the DPSCS data center and the network administered by ITCD that supports both ITCD and DPSCS. ITCD provides computing and network resources and operates as a computer services bureau for the DPSCS.

Our audit disclosed that password controls and controls over certain computer system and database files were not sufficient. In addition, critical firewalls were not configured to properly protect the DPSCS network from untrusted third parties.

DPSCS' response to the audit, on behalf of ITCD, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us by ITCD during the course of this audit.

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 Information Technology and Communications Division (ITCD) of the Department of Public Safety and Correctional Services (DPSCS) operates the DPSCS data center as a computer service provider for DPSCS operating agencies (for example, the Division of Correction). The ITCD provides data, information, and communications services to the DPSCS, criminal justice entities, and the public. In addition, the ITCD maintains application systems containing sensitive information, such as the Sex Offender Registry Database and the Maryland Automated Fingerprint Identification System, and operates a statewide computer network. Furthermore, the ITCD operates a wide area network (WAN) that connects with more than 200 statewide remote sites, such as local law enforcement agencies, and the DPSCS data center's local network. The DPSCS, through its WAN, offers its users access to various information technology services including mainframe computer-based applications (for example, the Criminal Justice Information System), database management, network services, email, and the Internet. Finally, the ITCD maintains the operating system and security software environment in which agency applications are executed. ITCD's fiscal year 2011 budget totaled approximately $38 million and provided funding for 247 authorized positions.

Our audit focused exclusively on the computer and network operations of the ITCD data center. An audit of the ITCD fiscal operations was conducted as part of the audit of the DPSCS Office of the Secretary, and a separate report was issued on September 15, 2010.

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 March 14, 2008. We determined that the ITCD satisfactorily addressed four of these six findings, and the remaining two findings are repeated in this report.

Findings and Recommendations

Network and Data Center Information Systems Security and Control

Background

The Maryland Department of Information Technology's (DoIT) *Information Security Policy* stipulates that all State agencies must ensure that information is accessed by the appropriate persons for authorized use only. To accomplish this, the Information Technology and Communications Division's (ITCD) computer systems contain security software that is capable of restricting access to system, security, 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 system to log onto various computer processing applications to update critical data files. Unauthorized requests are denied access by the security software. Furthermore, the ITCD's network devices can be configured to provide network security for network users.

ITCD operates numerous firewalls to protect critical network devices from untrusted third parties and from unwarranted access. These firewalls include internal firewalls protecting devices containing the most critical systems, external firewalls providing protection from external networks (for example, the Internet), and wide area network (WAN) firewalls protecting the internal network from untrusted third parties.

Finding 1
Controls over critical operating system and database files were not adequate.

Analysis

Procedures were not in effect to provide assurance that numerous critical operating system and database files were adequately protected. Specifically, we noted the following conditions:

- Numerous individuals had unnecessary modification access to five critical operating system libraries, which contained numerous system files. In several instances, this access was unlogged. A similar condition was noted in our two preceding audit reports.

- Unlogged modifications could be made to 70 critical operating system libraries. Accordingly, such modifications would not be subject to review and approval by supervisory personnel. A similar condition was noted in our two preceding audit reports.

- Several individuals had necessary, but unlogged, direct modification access to certain critical mainframe database programs and files.

These conditions could ultimately result in unauthorized changes to critical data files, many of which would not likely be detected by management.

Recommendation 1
We recommend that ITCD
a. remove unnecessary access to critical operating system files (repeat),
b. ensure that modifications to all critical operating system files are logged by security software (repeat), and
c. ensure that direct modification access to critical mainframe database programs and files is logged.

Finding 2
Mainframe and database password controls need improvement.

Analysis
Mainframe and database password controls need improvement. Specifically, we noted the following conditions:

- Eighty-nine mainframe user accounts were not required to have periodic password changes. As a result, compromised passwords could be used for extended periods. A similar condition was commented upon in our two preceding audit reports.

- Password length and complexity requirements were not enabled for two important databases. As a result, these passwords were susceptible to potential compromise.

The DoIT *Information Security Policy* specifies requirements for password lifetime periods, length, and complexity for State agencies.

Recommendation 2
We recommend that the ITCD adhere to the DoIT *Information Security Policy* password requirements (repeat).

Finding 3
There was a lack of assurance that the DPSCS network was properly secured.

Analysis

There was a lack of assurance that the DPSCS network was properly secured. We noted that the firewall rules on the internal, external, and wide area network firewalls allowed numerous unnecessary connections to portions of the DPSCS network, thereby placing various network devices at risk. For example, an untrusted third party had unnecessary network level access to several network devices used to manage the DPSCS network. ITCD personnel did not have an adequate understanding of firewall rules on its critical internal and external firewalls and, therefore, lacked assurance as to the adequacy of the rules on these firewalls and their ability to properly protect the DPSCS network.

Recommendation 3

We recommend that ITCD personnel obtain a comprehensive understanding of the firewall rules for all of the DPSCS firewalls and perform a detailed analysis of all firewall rules. Based upon this analysis, we recommend that ITCD configure its firewalls to achieve a "least privilege" security strategy giving individuals and devices only the access needed to perform necessary tasks.

Audit Scope, Objectives, and Methodology

We have audited the Department of Public Safety and Correctional Services (DPSCS) – Information Technology and Communications Division (ITCD). Fieldwork associated with our review of the Division was conducted during the period from November 2010 to July 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 the ITCD's internal control over the DPSCS data center and network, and certain Office of the Secretary applications and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support the DPSCS and its user agencies. ITCD's fiscal operations are audited separately as part of our audit of the DPSCS Office of the Secretary. The latest audit report on the Office of the Secretary was issued on September 15, 2010. We also determined the status of the findings contained in our preceding audit report dated March 14, 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, databases, firewalls, and routers. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of the ITCD's 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.

The ITCD's 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 ITCD's ability to operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to the ITCD that did not warrant inclusion in this report.

The DPSCS response, on behalf of the ITCD, 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 DPSCS regarding the results of our review of its response.

APPENDIX

Department of Public Safety and Correctional Services

Office of the Secretary
300 E. JOPPA ROAD • SUITE 1000 • TOWSON, MARYLAND 21286-3020
(410) 339-5000 • FAX (410) 339-4240 • TOLL FREE (877) 379-8636 • V/TTY (800) 735-2258 • www.dpscs.state.md.us

January 3, 2012

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits, Room 1202
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Myers:

The Department of Public Safety and Correctional Services has reviewed the draft audit report dated December 2011 for the Information Technology and Communication Division (ITCD). The Department appreciates the constructive recommendations that were made as the result of this audit. Be assured that appropriate corrective actions have been or will be implemented to ensure full compliance with each recommendation.

Attached is Chief Information Officer Brother's response to the draft audit report, with which I concur. Mr. Brothers will continue to implement corrective action to address all of the audit findings, and will closely monitor the status in order to prevent any repeat audit findings in the next audit.

I trust that these responses adequately address the findings and recommendations contained in the draft audit report. If you have any questions regarding the Department's responses, please contact me.

Sincerely,

Gary D. Maynard

Gary D. Maynard
Secretary

Attachment

c: G. Lawrence Franklin, Deputy Secretary for Administration, DPSCS
Ronald C. Brothers, Chief Information Officer, ITCD
Joseph M. Perry, Inspector General, DPSCS

Department of Public Safety and Correctional Services

Information Technology & Communications Division

Post Office Box 5743 • Pikesville, Maryland 21282-5743
Main №: 410-585-3100 • Facsimile №: 410-764-4035 • www.dpscs.maryland.gov

STATE OF MARYLAND

MARTIN O'MALLEY
GOVERNOR

ANTHONY G. BROWN
LT. GOVERNOR

GARY D. MAYNARD
SECRETARY

G. LAWRENCE FRANKLIN
DEPUTY SECRETARY
ADMINISTRATION

J. MICHAEL STOUFFER
DEPUTY SECRETARY
OPERATIONS

DAVID N. BEZANSON
ASSISTANT SECRETARY
CAPITAL PROGRAMS

RONALD C. BROTHERS
CHIEF INFORMATION
OFFICER

C. KEVIN COMBS
DEPUTY CHIEF
INFORMATION OFFICER

December 27, 2011

Gary D. Maynard, Secretary
Department of Public Safety & Correctional Services
300 East Joppa Road, Suite 1000
Towson, Maryland 21286

Via

G. Lawrence Franklin, Deputy Secretary
Department of Public Safety & Correctional Services
300 East Joppa Road, Suite 1000
Towson, Maryland 21286

Dear Secretary Maynard:

Enclosed is the Information Technology and Communications Division's (ITCD) response to the draft Legislative Audit report dated December 2011. This audit included an internal control review of the Department's data center and the network administered by ITCD that supports ITCD and the Department. The ITCD has begun, and will continue to pursue full implementation of all of the legislative auditor's recommendations.

Finding 1:
Controls over critical operating system and database files were not adequate.

Recommendation 1:
We recommend that ITCD

a. **remove unnecessary access to critical operating system files (repeat),**
b. **ensure that modifications to all critical operating system files are logged by security software (repeat), and**
c. **ensure that direct modification access to critical mainframe database programs and files is logged.**

We agree
ITCD has removed unnecessary modification access from the critical operating system libraries. New critical library files have been added to the mainframe audit file. Also, ITCD has added critical system files to mainframe security software. These files continue to be logged and reviewed weekly. In addition, a program is run each month to compare all dataset high-level qualifiers (HLQ) in the mainframe's master catalog with those in the alias exception report. ITCD will ensure that direct modification access to critical mainframe database programs and files continues to be logged and new files are added to mainframe security software.

Finding 2:
Mainframe and database password controls need improvement.

Recommendation 2:
We recommend that the ITCD adhere to the DoIT *Information Security Policy* password requirements (repeat).

We agree
ITCD will adhere to the DoIT Information Security Policy for password requirements. Training accounts in question have been deleted and services accounts needed to run applications within our environment have been modified for system-only access. ITCD is in the process of strengthening the password settings for all appropriate databases. The anticipated completion date is the end of February 2012.

Finding 3:
There was a lack of assurance that the DPSCS network was properly secured.

Recommendation 3:
We recommend that ITCD personnel obtain a comprehensive understanding of the firewall rules for all of the DPSCS firewalls and perform a detailed analysis of all firewall rules. Based upon this analysis, we recommend that ITCD configure its firewalls to achieve a "least privilege" security strategy giving individuals and devices only the access needed to perform necessary tasks.

We agree
ITCD personnel are obtaining a comprehensive understanding of the firewall rules for all DPSCS firewalls. Also, ITCD is currently performing a detailed analysis of DPSCS firewall rules. Old rules that have inadequate information are being disabled in preparation for permanent deletion as they are reviewed. In addition, ITCD is in the process of configuring its firewalls to achieve a "least privilege" security strategy. The anticipated completion date is the end of July 2013.

Please advise if you have any questions regarding the Division's responses to the audit report.

Sincerely,

Ronald C. Brothers
Chief Information Officer

RCB:tdp
cc: G. Lawrence Franklin, Deputy Secretary
Joseph M. Perry, Inspector General
File

AUDIT TEAM

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

Edwin L. Paul, CPA, CISA
Albert E. Schmidt, CPA
Information Systems Senior Auditors

Christopher D. Jackson
Jeffrey T. Zankowitz
Information Systems Staff Auditors