Audit Report

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

March 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

March 14, 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 Department of Public Safety and Correctional Services (DPSCS) - Information Technology and Communications Division (ITCD). Our audit included an internal control review of the DPSCS data center and the network administered by ITCD that supports ITCD and DPSCS.

Our audit disclosed that controls over certain computer programs and system and data files were not sufficient. Consequently, unauthorized changes could be made to critical user agency data such as arrest warrants and criminal history records. Also, critical network devices used to protect the internal network were not properly controlled and monitored.

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 the Department of Public Safety and Correctional Services (DPSCS)
Information Technology and Communications Division (ITCD)
March 2008

- **Access and monitoring controls over mainframe operating system files and database files were not adequate. For example, numerous employees had unnecessary, direct, modification access to many critical operating system files.**

  The ITCD should establish adequate access controls over operating system files and database files.

- **The Maryland Automated Fingerprint Identification System's (MAFIS) security settings, security reporting, password, and user account procedures were not adequate. For example, numerous accounts did not require passwords, passwords never expired, and accounts were not disabled after several invalid logon attempts.**

  The ITCD should enforce adequate security settings and provide for security event reporting of recorded accesses, access violations, and userid changes. In addition, password and user account procedures should be established in accordance with the Department of Budget and Management (DBM) *Information Technology Security Policy and Standards*.

- **A complete information technology disaster recovery plan did not exist.**

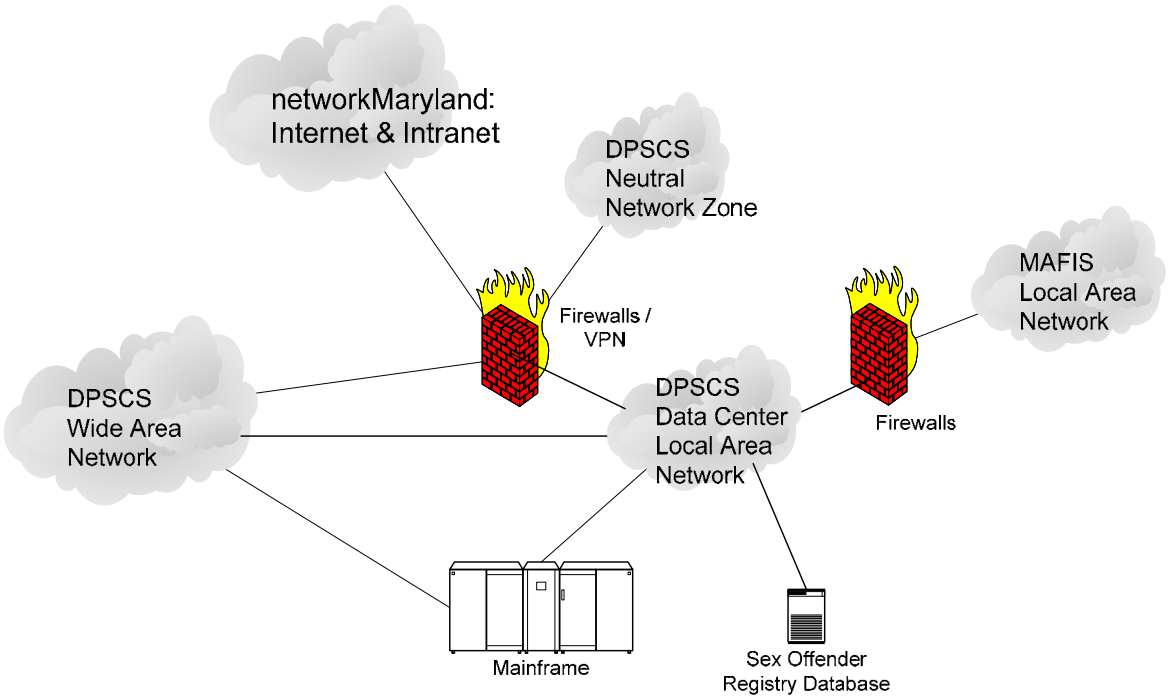
  The ITCD should, in accordance with the DBM *Information Technology (IT) Disaster Recovery Guidelines*, develop and implement a comprehensive information systems disaster recovery plan that covers all critical functions.

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 (MAFIS), and operates a statewide computer network. Furthermore, the ITCD operates a wide area network (WAN) that connects with over 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 IT 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 2008 budget totaled approximately $37.7 million and provided funding for 261 positions.

Overview of the ITCD Network Environment



Separate Audit

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 February 16, 2007.

Current Status of Findings From Preceding Audit Report

Our audit included a review to determine the current status of the nine findings in our preceding audit report dated August 27, 2004. We determined that the ITCD satisfactorily addressed four of these nine findings, and the remaining five findings are repeated in this report.

Findings and Recommendations

Network and Data Center Information Systems Security and Control

Security Background

The Department of Budget and Management (DBM) *Information Technology Security Policy and Standards* stipulate that all State agencies must ensure that information is accessed by the appropriate persons for authorized use only. To accomplish this, the ITCD's computer systems contain security software which 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 system to sign 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.

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

Analysis

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

- Numerous individuals had unnecessary, modification access to 59 critical operating system libraries, which contained numerous system files. In several instances, this access was unlogged. A similar condition was noted in our preceding audit report.

- Twelve library names were defined to the operating system and were assigned certain privileges which legitimately allowed any programs in those libraries to bypass security controls; however, the associated libraries did not exist. Consequently, an individual could create or use unauthorized libraries with these names, thereby obtaining the same critical privileges as the libraries defined to the system. A similar condition was noted in our preceding audit report.

- Unlogged modifications could be made to 63 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 preceding audit report.

- Although we were advised by management that reports of changes made to critical operating system files were reviewed, documentation of these reviews was not available for the period from June 12, 2006 through November 20, 2006. As a result, for this period, management lacked assurance that unauthorized changes had not occurred without its knowledge.

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

Recommendation 1
We again recommend that ITCD management remove unnecessary access to critical operating system files. We also again recommend that all names defined to the system for critical libraries which do not exist be deleted. Furthermore, we again recommend that modifications to all critical operating system files be logged by security software. Finally, we recommend that reviews of reports of changes to critical operating system files be documented by ITCD management and retained for future review.

Finding 2
Mainframe password authentication and account authorization procedures need strengthening.

Analysis
Password authentication and account authorization procedures on the mainframe system needed to be strengthened. Specifically, we noted the following conditions:

- One hundred forty-two accounts were not required to have periodic password changes. As a result, compromised passwords could be used for extended periods.

- The ITCD requires only a user's account identification, name, and date of birth to reset a password for a user's account. As a result, someone other than the user could easily obtain this information and then attain unauthorized access by obtaining a new password for an existing account.

Similar conditions were commented upon in our preceding audit report.

The DBM *Information Technology Security Policy and Standards* has requirements for password lifetime periods and password reset procedures for State agencies.

Recommendation 2
We again recommend that the ITCD adhere to the DBM *Information Technology Security Policy and Standards* password authentication and account authorization requirements for the ITCD mainframe computer users.

Finding 3
Controls over critical mainframe database files and programs need improvement.

Analysis
Seventeen database users had necessary, but unlogged, direct modification access to certain critical mainframe database files and programs and nine users had unnecessary, but logged, modification access to additional critical production database files and programs. In addition, we were advised that the database audit logs, for a critical database system, were not reviewed. Without proper access controls and adequate review of database security events, inappropriate modifications could be made to critical database files, such as Criminal Justice Information System files, without detection by management.

Recommendation 3
We recommend that access to critical mainframe database files and programs be limited to only those users whose jobs require such privileges and that all such accesses be logged. We further recommend that the ITCD regularly review database logging reports, investigate any unusual events, and document and retain the reviews.

Finding 4
Security controls over MAFIS and the Sex Offender Registry Database were not adequate.

Analysis
The security settings, security reporting, password, and user account procedures for the Maryland Automated Fingerprint Identification System (MAFIS) were not adequate to protect critical fingerprint data files. In addition, procedures for monitoring access to the Sex Offender Registry Database were inadequate. Our review of controls over these systems found the following deficiencies:

- Security key-switches on MAFIS minicomputers were not properly set or controlled. Each MAFIS minicomputer has a security key which can be set to either the "secure" or "normal" position. Twenty-eight minicomputers were set to "normal" which allowed the bypass of security controls. In addition, several minicomputers had the

key stored next to the minicomputer which would allow anyone to set the mode to "normal." Similar conditions were commented upon in our preceding audit report.

- Security reports of logged accesses, access violations, and userid changes were not generated for MAFIS minicomputers. A similar condition was commented upon in our preceding audit report. In addition, the sex offender registry database auditing capabilities were not enabled. These conditions could result in unauthorized or inappropriate activities (affecting the integrity of the system), which could go undetected by management.

- Password and account controls on the two critical MAFIS servers tested did not comply with minimum requirements of the *Information Technology Security Policy and Standards*, issued by the DBM. For example, minimum password lengths were not required, passwords never expired, password complexity and history requirements were not enforced, and accounts were not disabled after several invalid logon attempts. Furthermore, numerous accounts on these minicomputers did not require a password to access the system. Similar conditions were commented upon in our preceding audit report.

Recommendation 4
We again recommend that the ITCD implement appropriate security controls over the aforementioned systems. Accordingly, we made detailed recommendations to the ITCD which, if implemented, should provide adequate controls over these systems.

Finding 5
A complete information technology disaster recovery plan did not exist.

Analysis
The ITCD did not have a complete information technology disaster recovery plan for recovering from disaster scenarios (for example, a fire). Although DPSCS had developed a *Disaster Recovery Quick Plan*, we determined that the quick plan was incomplete as it did not adequately address certain requirements of DBM's *Information Technology (IT) Disaster Recovery Guidelines.* Specifically, the quick plan did not identify alternate site processing arrangements, disaster recovery team designations, and areas of team member responsibility. Also, the plan had not been tested. A similar condition was commented upon in our preceding audit report.

Without a complete disaster recovery plan, a disaster could cause significant delays (for an undetermined period of time) in restoring operations above and beyond the expected delays that would exist in a planned recovery scenario.

Recommendation 5
We again recommend that, in accordance with the aforementioned *Information Technology (IT) Disaster Recovery Guidelines*, the ITCD develop and implement a comprehensive information systems disaster recovery plan that covers all of the DPSCS critical functions. We also recommend that, at a minimum, the plan address the required items noted above.

Finding 6
Administration and monitoring of critical network devices need improvement.

Analysis
Administration and monitoring of critical network devices, capable of protecting the internal network from security risks, need improvement. Specifically, we noted the following conditions with respect to the primary firewalls and a core network device:

- Numerous individuals had unnecessary administrative access to these devices and an insecure connection protocol was utilized for administration of the core network device. Access rules for critical network devices should use a "least privilege" security strategy which gives individuals only those privileges needed to perform assigned tasks. Similar conditions were commented upon in our preceding audit report.

- Failed attempts to logon to the core network device were not recorded and administrators did not regularly review the logs for this device. In addition, no documentation of reviews performed was retained.

Recommendation 6
We again recommend that administrative access to critical network devices be limited to personnel requiring such access and that only secure connection protocols be enabled on these devices. In addition, we recommend that log files for critical network devices contain all failed attempts to log on to the devices, that these logs be reviewed on a daily basis, and that these reviews be documented and retained for audit verification.

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 data center was conducted during the period from November 2006 to June 2007. Additionally, fieldwork associated with our review of the network was conducted during the period from March 2007 to July 2007. The audit was conducted in accordance with generally accepted government auditing standards.

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, MAFIS system, 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 the audit of the DPSCS Office of the Secretary. The latest audit report on the Office of the Secretary was issued on February 16, 2007. We also determined the status of the findings contained in our preceding audit report.

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 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 conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect ITCD's ability to maintain reliable financial records, 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

STATE OF MARYLAND

MARTIN O'MALLEY
GOVERNOR

ANTHONY G. BROWN
LT. GOVERNOR

GARY D. MAYNARD
SECRETARY

G. LAWRENCE FRANKLIN
DEPUTY SECRETARY

DIVISION OF CORRECTION

DIVISION OF PAROLE AND PROBATION

DIVISION OF PRETRIAL DETENTION AND SERVICES

PATUXENT INSTITUTION

MARYLAND COMMISSION ON CORRECTIONAL STANDARDS

CORRECTIONAL TRAINING COMMISSION

POLICE TRAINING COMMISSION

MARYLAND PAROLE COMMISSION

CRIMINAL INJURIES COMPENSATION BOARD

EMERGENCY NUMBER SYSTEMS BOARD

SUNDRY CLAIMS BOARD

INMATE GRIEVANCE OFFICE

March 10, 2008

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

Dear Mr. Myers:

The Department of Public Safety and Correctional Services has reviewed the February 26, 2008, draft audit report on the Department's Information Technology and Communications Division (ITCD). The Division as well as the Department acknowledge the importance of each finding and appreciate the constructive recommendations made as a result of this audit. I am pleased that Chief Information Officer Ronald C. Brothers reports that corrective action has already been implemented for many of the audit recommendations and that substantive progress has been made on the remaining recommendations.

It should be noted that during this audit period, there have been significant initiatives by the Division that were designed to improve customer service to Maryland's citizens by increasing economy and efficiency, creating safer communities, and enhancing relationships with local governments and other stakeholders that share a mutual vision. The Department is proud of the record of accomplishments for the Division and continues to strongly support its ongoing efforts to develop, administer, and deliver quality services to the people that it serves. Some significant recent accomplishments/initiatives include:

- Network Livescan - Network Livescans have been installed at five Hazmat locations. This equipment is used to process the identification and background checks for individuals applying for Commercial Driver's Licenses. In 2007, the use of these Livescans was expanded to also include applicant processing. Applicant processing is available at 25 applicant sites in addition to the 5 Hazmat sites. This equipment is used to process background checks for various licenses such as child care and nursing. Prior to the Livescans for applicant processing, customer responses were taking an average of 64 days for delivery. After implementation, the average response time has been reduced to three days. In addition, criminal processing has been installed at 62 locations. Livescans have enabled an average response time of 20 minutes for the rapid, positive identification of criminal suspects.

- Maryland Online Sex Offender Registry (MOSOR) - The automation of the MOSOR has provided a more rapid update of the registry by local law enforcement units, the ability to share the data with the National Registry and the FBI, and improved tools for the public to access the MOSOR information. Digital cameras were provided to local law enforcement units so the sex offender's picture can be posted with his/her information on the website. Local law enforcement units input the sex offender information into the automated system for validation by the Criminal Justice Information System's MOSOR information unit. This eliminates the time lapse between the local law enforcement units gathering the information and mailing it to the State for posting. Since the MOSOR information data is electronically stored, FBI files are updated immediately via electronic data sharing. The MOSOR information website is available for public viewing either by date of updated information or zip code. A graphic interface has been created to permit the public to view the location of registered sex offenders in relationship to specific communities or locations such as churches or schools. A service is also available to the public to provide either phone or email notice when there is sex offender movement within their community, and to provide a victim with phone or email notice when a specific sex offender changes location, is released by an institution, or is arrested.

- Uniform Fingerprinting of Offenders - Through the use of automated forms and installation of Livescan equipment, 13 Division of Parole and Probation sites were updated to record the entry into Parole and Probation as a reportable event. This also provided a means for capturing the offender's fingerprints for positive identification, as well as capturing a picture for the case manager's records. Many of the manual forms that were shared by the Maryland Parole Commission, the Division of Correction, and the Division of Parole and Probation have been automated by this project, eliminating the need for duplicative data entry and reducing the risk of error.

Attached is Chief Information Officer Ronald C. Brothers' response to the draft audit report, with which I concur. I trust that this adequately responds to your request. If you have any questions concerning this correspondence, please contact me.

Sincerely,

Gary D. Maynard
Secretary

Attachment
c: G. Lawrence Franklin, Deputy Secretary, DPSCS
Thomasina Hiers, Acting Chief of Staff, DPSCS
Ronald C. Brothers, ITCD Chief Information Officer, DPSCS
Susan Dooley, Director, Financial Services, DPSCS
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.state.md.us

STATE OF MARYLAND

MARTIN O'MALLEY
GOVERNOR

ANTHONY G. BROWN
LT. GOVERNOR

GARY D. MAYNARD
SECRETARY

G. LAWRENCE FRANKLIN
DEPUTY SECRETARY

RONALD C. BROTHERS
CHIEF INFORMATION
OFFICER

C. KEVIN COMBS
DEPUTY CHIEF
INFORMATON OFFICER

March 10, 2008

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

VIA

Thomasina Hiers, Acting Chief of Staff
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 February 26, 2008. 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 aggressively pursue full implementation of all of the legislative auditor's recommendations.

Finding # 1 - Controls over critical operating system files were not adequate.

We agree. ITCD has removed unnecessary access to critical operating system files. ITCD has also deleted all names defined to the system for critical libraries which do not exist. ITCD is also logging all modifications to all critical operating system files with security software. ITCD is also documenting and retaining the reviews of the reports that track changes to critical operating system files.

Finding # 2 - Mainframe password authentication and account authorization procedures need strengthening.

We agree. By December 31, 2008 ITCD will adhere to the DBM Information Technology Security Policy and Standards password authentication and account authorization requirements for the ITCD mainframe computer users.

Finding # 3 - Controls over critical mainframe database files and programs need improvement.

We agree. ITCD has limited access to critical mainframe database files and programs to only those users whose job requires such privileges and is logging all such accesses. ITCD is also regularly reviewing the database logging reports, investigating any unusual events, and documenting and retaining the reviews.

Finding # 4 - Security controls over MAFIS and the Sex Offender Registry Database were not adequate.

We agree. ITCD is currently implementing a new MAIFS system that will replace the current outdated system. The new system is slated to come online in 2008. ITCD has corrected the logging issues with the Sex Offender Registry and by July 31, 2008 will implement the OLA recommendations to provide adequate control over the Sex Offender systems.

Finding # 5 - A complete information technology disaster recovery plan did not exist.

We agree. ITCD has tried unsuccessfully for the past three years to obtain funding to implement a Disaster Recovery site. ITCD has investigated numerous "free solutions", but none have proved to be viable. ITCD is currently updating its written Disaster Recovery plan and will have this completed by the 2nd quarter of 2008.

Finding # 6 - Administration and monitoring of critical network devices need improvement.

We agree. ITCD has limited administrative access to critical network devices to only personnel requiring such access and will only enable secure connection protocols on these devices. In addition, ITCD is logging critical network devices for all failed attempts to log on to those devices, as well as reviewing the logs daily and documenting and retaining all reviews for audit verification.

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

c: G. Lawrence Franklin, Deputy Secretary
Joseph M. Perry, Inspector General
File

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

David J. Burger
Amanda L. Trythall
Information Systems Staff Auditors