



# AUDITOR GENERAL

## WILLIAM O. MONROE, CPA



### DEPARTMENT OF LAW ENFORCEMENT FLORIDA CRIME INFORMATION CENTER Information Technology Audit

#### Summary

The Department of Law Enforcement (Department) maintains the Florida Crime Information Center (FCIC). FCIC is an intrastate telecommunications network that provides agency-to-agency communication and access to computerized criminal justice information at the local, State, and Federal levels. FCIC provides, on a State level, information on wanted or missing persons, stolen property, domestic violence injunctions, parole status, deported aliens, and registered sexual predators.

The scope of this audit focused on evaluating selected information technology (IT) functions and determining the effectiveness of general and application controls applicable to FCIC during the period December 2002 through April 2003.

As described below, we noted deficiencies in certain general controls related to FCIC.

**Finding No. 1:** Improvements were needed in the documentation of program changes made to FCIC. In addition, the Department did not independently review or monitor program move activity.

**Finding No. 2:** Improvements were needed in the Department's IT risk management practices and in certain security controls protecting FCIC.

#### Background

The Department provides services in conjunction with local, State, and Federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. Florida law<sup>1</sup> provides the authority for the Department to conduct its operations within five main programs.

One such program is the Criminal Justice Information Program, which maintains a Statewide communication system and databases that allow criminal justice agencies to access and share State maintained criminal history information. These databases are made accessible to criminal justice agencies statewide through the FCIC network, which also links agencies to the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) network.

The Department's Information Resource Management (IRM) operates the FCIC as a round-the-clock network that allows Florida's criminal justice community to share critical information. Criminal justice agencies using FCIC include Federal offices, State offices (including State attorney offices), county offices (including sheriff's offices), local offices (including police departments), and other correctional offices.

<sup>1</sup> Section 943.05, Florida Statutes

NCIC provides criminal justice information (for example, criminal record history information, fugitives, stolen properties, missing persons) for both Federal and State crimes. NCIC serves criminal justice agencies in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, and Canada, as well as Federal agencies with law enforcement missions.

During our audit, we noted instances of deficiencies in computer general controls applicable to FCIC. These deficiencies and related recommendations are discussed in the following findings.

---

---

**Finding No. 1:  
Program Change Controls**

---

---

Good IT control practices dictate that procedures should be established to minimize the opportunity for application programmers and users to make unauthorized changes to production programs, job control language, and system software packages, thus compromising the integrity of the program source code and the results of processing. The objectives of program change controls and system development controls include, among other things, adequate user involvement in requesting, testing, and approving program changes; appropriate audit trails, including program change history logs (library management software); information systems and user personnel approval for program changes; and sufficient documentation of program changes. The objectives also include controlled production transfer procedures that reduce the risk of programmers having the ability to introduce unapproved test versions of programs into the production environment.

During our audit we noted that, contrary to Department procedures, none of the 10 program changes we reviewed had documentation available indicating that the developer was notified when installation was completed. Furthermore, there was no documentation available indicating who actually moved the programs into the production environment.

Also, there was no independent review and monitoring of program move activity. A report existed that identified the program moved into production, including the program name, date of move, and developer; however, individual moves could not always be cross-referenced to a program change request.

Without adequate program change control documentation and monitoring, there is an increased risk that unauthorized, unapproved, and untested changes will be made to FCIC and go undetected.

---

---

**Recommendation:**

---

---

**The Department should enhance the documentation of scheduled program moves into production to include the individual responsible for the move and the subsequent notification to the developer. In addition, the movement of FCIC programs to the production environment should be independently reviewed and monitored to ensure that only authorized programs are moved into production.**

---

---

---

---

**Finding No. 2:  
Risk Management Practices and Security Controls**

---

---

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources.

During our audit, we identified deficiencies in the Department's IT risk management practices and in certain control features implemented by the Department. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising Department information. However, the appropriate Department personnel have been notified of the deficiencies.

---

---

**Recommendation:**

**The Department, together with the State Technology Office should enhance its IT risk management practices. Additionally, the Department should implement the appropriate security control features to enhance the safeguarding of FCIC data, programs, and resources.**

---

---

---

---

**Other Matters**

---

---

**Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

HIPAA<sup>2</sup> addresses data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic data interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002, but the deadline may be extended to October 16, 2003, by filing an extension request. The final Privacy Rule was incorporated as a Federal regulation and compliance was required by April 14, 2003. The final Security Rule was incorporated as a Federal regulation and compliance is required by April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance.

In response to our inquiry regarding the HIPAA legislation, the Department provided us a copy of a letter from the Department's General Counsel to its Chief Information Officer dated December 11, 2002. This letter stated that HIPAA did not apply to Department operations. The letter also stated that further development and interpretation of rules by the United States Department of Health and Human Services may require the Department to revisit this opinion some time in the future.

---

---

**Scope, Objectives, and Methodology**

---

---

The scope of this audit focused on evaluating selected IT functions applicable to FCIC during the period December 2002 through April 2003. Our objectives were to determine the effectiveness of selected general and application controls related to FCIC and to determine management's awareness of the HIPAA legislation and what actions, if any, have been taken concerning this legislation.


In conducting the audit, we interviewed appropriate Department personnel, observed Department processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to FCIC.

---

<sup>2</sup> Public Law 104-191

**Authority**

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

  
William O. Monroe, CPA  
Auditor General

**Auditee Response**

In response letters dated December 16, 2003, and December 17, 2003, respectively the Chief Information Officer for the State Technology Office and the Department's Commissioner generally concurred with our audit findings and recommendations. The Chief Information Officer's and Commissioner's responses can be viewed in their entirety on the Auditor General Web site.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in Government Auditing Standards issued by the Comptroller General of the United States. This audit was conducted by Wayne Revell, CISA, and supervised by Tina Greene, CPA\*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA\*, CISA, Audit Manager, via e-mail at [joningram@aud.state.fl.us](mailto:joningram@aud.state.fl.us) or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.state.fl.us/audgen>); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

\*Regulated by State of Florida.



Florida Department of  
Law Enforcement

Guy M. Tunnell  
Commissioner

Post Office Box 1489  
Tallahassee, Florida 32302-1489  
(850) 410-7001  
<http://www.fdle.state.fl.us>

Jeb Bush, *Governor*  
Charlie Crist, *Attorney General*  
Tom Gallagher, *Chief Financial Officer*  
Charles H. Bronson, *Commissioner of Agriculture*

December 17, 2003

Mr. William O. Monroe, CPA  
Auditor General  
G74 Claude Pepper Building  
111 West Madison Street  
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

We have received the preliminary and tentative findings and recommendations from the following information technology audit of:

**Florida Department of Law Enforcement  
Florida Crime Information Center  
For the Period December 2002 through April 2003**

Your findings and our related explanations or our descriptions of actual or proposed corrective actions initiated by the Florida Department of Law Enforcement are enumerated below:

**Finding No. 1**

**The Department should enhance the documentation of scheduled program moves into production to include the individual responsible for the move and the subsequent notification to the developer.**

**FDLE Response:**

Agree. It has been the practice of IRM to announce in the daily status meetings when items approved our internal review board (CCCB) will be installed. However, no individual notification was given to the developer after the implementation into the production environment. On November 25, 2003 a new procedure was implemented in IRM. In conjunction with the new procedure, the CCCB Checklist form was changed and all IRM members were notified of the new procedures.

- CCCB Checklist – added lines for name and signature of individual implementing change into production
- CCCB Checklist – added lines for date and time of change implementation
- CCCB Checklist – added lines for documenting notification to developer

As IRM revises the CCCB Process, notification of the developer and documentation of the installation will be retained.

**Finding No. 1 Continued**

**In addition, the movement of FCIC programs to the production environment should be independently reviewed and monitored to ensure that only authorized programs are moved into production.**

FDLE Response:

Agree. During the time of the audit, IRM was in transition phase where a contractor (DCI) had responsibility for some development and had access to the production environment. That no longer is the case, nor is it our common practice. The Production Systems Section, acting as the CCT, moves all code into production on FCIC. Members of that section are neither developers nor are they in the formal review and approval process.

By definition, a Change Control Trustee (CCT) role is to implement equipment and software changes in the production environment independent of the development and review process.

To address independent review and monitoring, IRM will research options for improving traceability of programs moved into production. Specifically, IRM will identify additional information to be captured in system logs that will enable an independent reviewer to trace back to earlier steps in the software development and approval process and will implement procedures for post-implementation review. Recommendations will be developed and submitted to the CIO within the next 90 days.

Finding No. 2

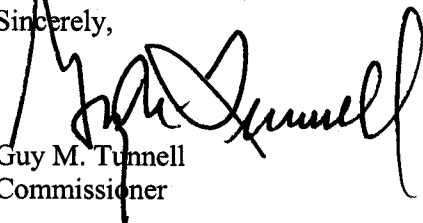
**The Department, together with the State Technology Office should enhance its IT risk management practices. Additionally, the Department should implement the appropriate security control features to enhance the safeguarding of FCIC data, programs, and resources.**

FDLE Response:

Agree. From the early days of the FCIC system (more than 30 years ago), the Department has been committed to securing the FCIC system from unauthorized access, misuse and abuse. As laws, policy, user requirements and technologies evolve, the Department implements and adapts security measures to protect the system. The Department recognizes that this is a continuous process. The Department will work with State Technology Office to enhance IT risk management practices. The Department will implement additional security control features to further safeguard the FCIC system. The Chief Information Officer will submit specific recommendations to the Commissioner and Executive Policy Board regarding additional security controls. Contingent on approval by the Commissioner and Executive Policy Board, recommendations will be implemented.

The observations and recommendations in your audit report are appreciated. If you require any further information regarding the actual or proposed corrective actions, please contact me or Inspector General Leon Lowry at 410-7225.

Sincerely,



Guy M. Tunnell  
Commissioner

GMT/ALL/dkk