




Florida Department of  
Law Enforcement

Gerald M. Bailey  
Commissioner

Office of Inspector General  
Post Office Box 1489  
Tallahassee, Florida 32302-1489  
(850) 410-7000  
www.fdle.state.fl.us

Rick Scott, Governor  
Pam Bondi, Attorney General  
Jeff Atwater, Chief Financial Officer  
Adam Putnam, Commissioner of Agriculture

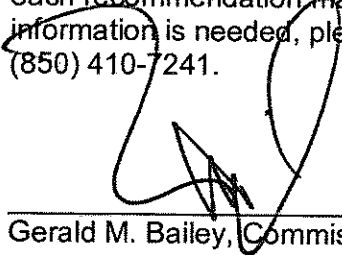
**MEMORANDUM**

**DATE:** April 29, 2013  
**TO:** Gerald M. Bailey, Commissioner  
Office of the Executive Director  
**VIA:** Dean Register, Assistant Inspector General   
Office of Inspector General  
**FROM:** Al Dennis, Inspector General  
Office of Inspector General  
**SUBJECT:** Six-month Status Report  
Auditor General Report Number 2013-030  
Department of Law Enforcement  
Information Technology Operational Audit

---

In accordance with the provisions of Section 20.055 (5)(h), Florida Statutes, we present the six-month status report on  
Auditor General Report, Number 2013-030  
Department of Law Enforcement  
Florida Crime Information Center (FCIC) and  
Computerized Criminal History System (CCH)  
Information Technology Operational Audit

The report details the implementation or status of corrective actions taken by the Department for each recommendation made in the above referenced Auditor General report. If further information is needed, please contact me or Director of Auditing Lourdes Howell-Thomas at (850) 410-7241.

  
\_\_\_\_\_  
Gerald M. Bailey, Commissioner

4.30.13  
\_\_\_\_\_  
Date

AD/lht

Attachment

cc: Kathy DuBose, Coordinator  
Joint Legislative Auditing Committee

**Auditor General Report Number 2013-030**  
**Department of Law Enforcement**  
**Information Technology Operational Audit**  
**Six-Month Status Report**

**Finding #1 – Appropriateness of Access Privileges**

The access privileges of some employees and contractors were not necessary for the users' assigned job responsibilities and did not enforce an appropriate separation of duties. Additionally, some active user accounts existed with no identifiable owners and were no longer being used by the Department.

**Recommendation:**

The Department should limit access privileges to only what is needed to perform job responsibilities. The Department should also evaluate employee job responsibilities relating to Florida Crime Information Center (FCIC) and Computerized Criminal History System (CCH) and make appropriate changes to enforce an appropriate separation of incompatible duties (e.g., development staff having update privileges in the application).

Additionally, the Department should deactivate any user accounts that are no longer being used.

**6 Month Status Report:**

- The Department has modified access privileges for all accounts identified in the audit as having inappropriate levels of access.
- The Department immediately deactivated user accounts that were identified as belonging to individuals who had separated from employment and continues to take appropriate action for members who separate from the agency.
- The Department has patched a programming flaw in CCH to prevent users from performing expunction-related modifications for which they are not authorized.
- The Department continues a comprehensive review of accounts and access levels in FCIC and CCH. This review is scheduled to be completed in May 2013.

---

**Finding #2 – Access Documentation and Management**

Authorization documentation for the access privileges of some users was missing or incomplete. Additionally, the Department lacked written procedures for managing access to CCH; and FCIC access management process needed improvement.

**Recommendation:**

The Department should maintain complete documentation of management authorization, including authorization signatures, for user access that specifies the access privileges assigned to the users.

Additionally, the Department should develop written procedures for managing access to CCH and enhance FCIC procedures to address the management of elevated levels of access privileges.

### **6 Month Status Report:**

- The Department has revised the agency policy (FDLE Policy 2.5) regarding access to information systems. The revision was completed in March 2013 and is scheduled for adoption at the Command Staff meeting in June 2013. The policy contains procedures and requirements for the administration of access to all FDLE information systems, which include FCIC and CCH.
  - The Department's Criminal Justice Information Services (CJIS) program has modified the access request form for CCH to include documentation of elevated access privileges. The request form for CCH is in addition to the requirements set forth in Policy 2.5 and will take effect September 2013.
- 

### **Finding #3 – Timely Deactivation of Access Privileges**

The Department did not timely deactivate the access privileges of some former employees. Similar issues were communicated to Department management in connection with our report No. 2004-071.

#### **Recommendation:**

The Department should enhance its periodic reviews and follow-up of access privileges to ensure that the access privileges of all former employees to FCIC and CCH are deactivated in a timely manner.

### **6 Month Status Report:**

- Included in the aforementioned revision of the Department's Policy 2.5 is a procedure that directs Application Access Administrators to review monthly Employee Status Reports for any member affected by personnel actions (promotion/transfer/demotion, separation, etc.) and modify permissions and/or terminate access to the CCH system as appropriate.
  - CJIS incorporated the Department's draft Policy 2.5 as it relates to Application Access Administration for deactivating member access to FCIC through the eAgent application when affected by a qualifying personnel action. This process is already in effect for both FCIC and CCH. As noted in the original audit response, CJIS Certification is valid for two years from certification date and this procedure does not affect that certification.
- 

### **Finding #4 – Periodic Review of Access Privileges**

The Department did not perform comprehensive periodic reviews of the appropriateness of user access privileges or logs of changes to database access privileges. Similar issues were communicated to Department management in connection with our report Number 2004-071.

#### **Recommendation:**

The Department should ensure that comprehensive reviews of FCIC and CCH access privileges and change logs are conducted on a periodic basis.

## **6 Month Status Report:**

- Included in the aforementioned revision of the Department's Policy 2.5 is a procedure that directs Application Access Administrators to review monthly Employee Status Reports for any member affected by personnel actions (promotion/transfer/demotion, separation, etc.) and modify permissions and/or terminate access to FCIC (through the eAgent application) and the CCH system as appropriate.
  - The Department has not yet finalized the most effective mechanism to complete reviews of FCIC Database user access privilege logs. We are currently assessing available options and expect to have a solution implemented by September 2013.
- 

## **Finding #5 – Other Security Controls**

Certain Department security controls needed improvement in the areas of risk management, user authentication, operating system access, network session controls, physical access to IT resources, assessing vulnerabilities, software patch management, and safeguarding confidential and exempt information. One of these issues was communicated to Department management in connection with our report Number 2004-071.

### **Recommendation:**

The Department should improve security controls in the areas of risk management, user authentication, operating system access, network session controls, physical access to IT resources, assessing vulnerabilities, software patch management, and safeguarding confidential and exempt information to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

## **6 Month Status Report:**

Due to the sensitive nature of this finding, the Department has not documented specifics in this status update; however, the Department is actively working toward mitigating the noted deficiencies. Several of the most pressing items have already been fully mitigated, and efforts to mitigate the complement are progressing well. The Department anticipates that all pending activities will be complete prior to October 2013.

---

## **Finding #6 – Program Change Management**

The Department did not perform post-implementation reviews to ensure that only authorized FCIC and CCH changes had been moved into the production environment. A similar finding with regard to the movement of FCIC programs into the production environment as noted in our report Number 2004-071.

### **Recommendation:**

The Department should implement a process for monitoring the movement of FCIC and CCH program changes into the production environment to ensure that unauthorized or erroneous changes, should they occur are timely detected.

## **6 Month Status Report:**

In the Department's initial response to the Auditor General's report, the agency agreed processes can always be improved, but did not concur with the audit's assessment of the code management process for CCH. Furthermore, the Department indicated that any activity related to modifying the code management process for FCIC would be assigned a low priority as compared to other mitigation activities. At this time, activity on this recommendation is still pending and will be pursued as time and resources permit.

---

## **Finding #7 – Use of SSNs**

Contrary to Section 119.071(5)(a)2.a, Florida Statutes, the Department collected and used certain employee social security numbers (SSNs) in FCIC and CCH without specific authorization in law or without having established the imperative need to use the SSN for the performance of its duties and responsibilities as prescribed by law.

### **Recommendation:**

In the absence of establishing an imperative need for the use of certain employee SSNs, the Department should comply with State law by establishing another number to be used in FCIC and CCH rather than the SSN.

## **6 Month Status Report:**

Due to the sensitive nature of this finding, the Department has not documented specifics in this status update; however, the Department took the recommendation under advisement and has implemented changes as deemed appropriate for those systems in which it was feasible.

---

## **Finding #8 – Disaster Recovery and Backup Controls**

The Department<sup>1</sup> had not annually tested its Continuity of Operations Plan (COOP) and lacked some backup tape controls.

### **Recommendation:**

The Department should annually test the effectiveness of the COOP. The Department should also periodically test the recoverability of data from backup tapes and implement a mechanism to track the physical movement of backup tapes.

## **6 Month Status Report:**

- At the conclusion of the audit period, the Office of Information Resource Management reviewed its existing COOP and concluded that it required significant revision in advance of an annual test. A preliminary revision was submitted to the Department's Emergency Coordination Officer (ECO) per statutory requirements in January, 2013. A final revision of the COOP is currently underway but is not projected to be completed before October, 2013.

---

<sup>1</sup> Although the term "Department" is used in the audit report, this finding refers specifically to the COOP covering the Office of Information Resources Management.

This is due to the extensive effort being invested in revisiting business impact analyses, application and data categorization, disaster recovery capabilities, and cost-benefit studies.

- In support of the effort to revise the IRM COOP, the Department's Information Security Manager (ISM) recently attended a 16 hour training seminar covering business continuity management planning and disaster recovery planning. This training will help to ensure the most up-to-date principles and best practices are applied to the revision.
- The Chief Information Officer (CIO) has directed the Chief of Production Systems to design, coordinate, and carry out a full failover test of FCIC, CCH, and related systems as described in the COOP. Full failover testing of FCIC and CCH must be approached with extreme caution due to the potential impacts on public safety, specifically to law enforcement and criminal justice agencies and the requirement for their uninterrupted access to these systems. Local law enforcement agencies would experience a significant reduction in processing capacity and availability to access criminal history, warrants, violent gang and terrorist organization files, and other such information contained within these systems during a failover test. Therefore, the Department will need to coordinate with state and national law enforcement entities in advance of a test. Furthermore, a considerable investment in the planning process to avoid unexpected complications and to ensure a return to full service can be accomplished quickly in the event of an unsuccessful test. At this time, a firm date for testing has not been established but is anticipated before the end of the calendar year.
- The operational group responsible for managing backup tapes is collaborating with the Department's ISM to assess current procedures for tape handling and to devise a procedure for regular tape testing. Due to resource constraints, level of effort and costs to construct a suitable test environment, further research and planning are required before a full scale test can be performed. At this time, a completion date for a backup tape test is pending but is anticipated before the end of the calendar year.