REPORT NO. 2013-030
OCTOBER 2012

DEPARTMENT OF LAW ENFORCEMENT

FLORIDA CRIME INFORMATION CENTER (FCIC)
AND
COMPUTERIZED CRIMINAL HISTORY SYSTEM (CCH)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DEPARTMENT OF LAW ENFORCEMENT

Pursuant to Section 20.201(1), Florida Statutes, the Executive Director of the Department of Law Enforcement is appointed by the Governor with the approval of three members of the Cabinet and is subject to confirmation by the Senate. Commissioner Gerald M. Bailey served as Executive Director during the period of audit.

The audit team leader was Daniel Pearce, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CITP, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF LAW ENFORCEMENT

Florida Crime Information Center (FCIC)
and
Computerized Criminal History System (CCH)

SUMMARY

The Department of Law Enforcement (Department) maintains the Florida Crime Information Center (FCIC) and Computerized Criminal History system (CCH). FCIC serves as a central system providing criminal justice agencies with access to Federal, State, and local criminal justice information, including wanted persons, missing persons, stolen property, and criminal records. CCH serves as the State's central repository for criminal record information, such as arrests, dispositions, and incarceration records in Florida. Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to FCIC and CCH. The results of our audit are summarized below:

Finding No. 1: 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.

Finding No. 2: 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 procedures needed improvement.

Finding No. 3: 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.

Finding No. 4: 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 No. 2004-071.

Finding No. 5: 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 No. 2004-071.

Finding No. 6: The Department did not perform post-implementation reviews to ensure that only authorized FCIC and CCH program changes had been moved into the production environment. A similar finding with regard to monitoring the movement of FCIC programs into the production environment was noted in our report No. 2004-071.

Finding No. 7: 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.

Finding No. 8: The Department had not annually tested its Continuity of Operations Plan (COOP) and lacked some backup tape controls.

BACKGROUND

The Department's mission is to promote public safety and strengthen domestic security by providing services in partnership with local, State, and Federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. The Department's Criminal Justice Information Program maintains the central repository of criminal history records for the State of Florida in the Computerized Criminal History system

(CCH), as well as databases in the Florida Crime Information Center (FCIC) that provide data such as wanted and missing persons, stolen vehicles, guns and property, and domestic violence injunctions. These databases are made accessible to all criminal justice agencies Statewide through FCIC, which also links agencies to the Federal Bureau of Investigation's National Crime Information Center. The Office of Information Resource Management (IRM) is responsible for maintaining the technical infrastructure supporting all FDLE systems, including FCIC and CCH.

As noted in our report No. 2004-161, the Department had planned to replace CCH and the Automated Fingerprint Identification System (AFIS) with a new application, the Integrated Criminal History System (ICHS), with full implementation projected for December 2005. However, the ICHS project was transitioned to the FALCON ICHS project in mid-2004. AFIS was replaced by FALCON, but additional planned functionality for FALCON to replace CCH was not funded by the Legislature for 2008-09 or subsequent years. The Department continued to use CCH as its repository for criminal history records during the period of our audit.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Appropriateness of Access Privileges

Effective security controls include logical access controls that limit user access privileges to only what is needed in the performance of assigned job responsibilities and enforce an appropriate separation of incompatible duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(3), Florida Administrative Code, provides that workers, including employees, contractors, and other persons whose conduct is under the direct supervision of an agency, shall be authorized access to agency IT resources based on the principles of "least privilege" (the principle that grants the minimum possible privileges to permit a legitimate action) and "need to know" (the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties). AEIT Rule 71A-1.007(5), Florida Administrative Code, provides that, for functions susceptible to fraudulent or other unauthorized activity, an agency shall ensure separation of duties so no individual has the ability to control the entire process.

Our review of the appropriateness of access privileges within the FCIC and CCH applications and related IT resources disclosed that some users, including current Department employees and contractors, had update access privileges that were not necessary for their 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. These conditions, described below in Table 1, increased the risk of errors, fraud, misuse, or other unauthorized modification of Department data.

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

Table 1

Review of FCIC and CCH Access Privileges	FCIC Application Access – End-User	FCIC Application Access – Application Programmers	Direct Access to FCIC Database	CCH Application Access – End-User	CCH Application Access – Application Programmers	Direct Access to CCH Systems Software	Direct Access to CCH Database	Access to CCH Source Libraries	Access to Move CCH Programs into Production
Access Tested as of	12-13-2011	12-13-2011	12-9-2011	12-19-2011	12-19-2011	12-19-2011	12-9-2011	1-12-2012	1-12-2012
Accounts Reviewed by Auditor	**20**	**23**	**10**	**33**	**16**	**12**	**5**	**16**	**16**
Accounts with Unnecessary Access	1	0	0	21	0	0	0	0	0
Accounts Allowing Incompatible Duties	0	19	0	0	4	1	2	4	1
Accounts Without an Identifiable Owner	0	0	3	0	0	2	0	0	0
Total Accounts with Inappropriate Access	**1**	**19**	**3**	**21**	**4**	**3**	**2**	**4**	**1**

Through additional audit procedures, we identified other inappropriate access privileges. Specifically:

- Our comparison of users with FCIC database access privileges as of December 9, 2011, to their FCIC application access privileges disclosed that one developer had FCIC application access privileges, contrary to an appropriate separation of developer and end-user duties.
- In FCIC, 52 users had been granted administrative functions such as changing access privileges. The sensitive nature of the administrative functions and the large number of users with access to such functions indicated a need for the Department to review the necessity of the access privileges.
- A programming flaw existed within the CCH application that allowed any user with inquiry or update access to any one function within the Expunge Subsystem to have update access to all functions available within the Expunge Subsystem. As of March 5, 2012, 67 users had access to functions within the Expunge Subsystem that were not explicitly granted. Our review of CCH transactions dated from September 1, 2011, through December 31, 2011, disclosed that only users whose job responsibilities included sealing and expunging records had performed these functions. Nevertheless, the risk of unauthorized Expunge Subsystem transactions would be reduced if access was restricted to only those users whose assigned job responsibilities included executing such transactions.

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 FCIC and 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.

Finding No. 2: Access Documentation and Management

AEIT Rule 71A-1.007(1), Florida Administrative Code, provides that information owners shall be responsible for authorizing access to information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. The effectiveness of access controls are also enhanced by the establishment of written procedures that describe management's expectations for assigning, monitoring, and deactivating access privileges.

All FCIC users were required to successfully complete Criminal Justice Information Services certification training before being granted unsupervised access to FCIC. Completion of an FCIC user's required certification in the

Training Information System represented authorization for the default level of FCIC access privileges. However, the Department did not maintain complete documentation of authorization for elevated levels of FCIC access privileges.

We requested access authorization documentation for the 33 users with CCH application access described previously in Finding No. 1 to determine if access granted was adequately documented and authorized. For 9 of the 33 user accounts, authorization documentation for the user access privileges did not exist. Our review of the 24 access authorization documents that were in the Department's records disclosed that 4 of the documents were missing authorization signatures for CCH access and 20 of the documents did not specify which access privileges had been assigned to the users. As indicated by the inappropriate access privileges described previously in Finding No. 1, the lack of complete and specific documentation of management's authorization of user access privileges may limit the Department's ability to ensure that user access privileges granted to employees and contractors do not exceed what is necessary for the accomplishment of assigned job responsibilities.

Our audit further disclosed that the Department lacked written procedures for managing (i.e., assigning, monitoring, and deactivating) access to CCH. The Department had developed a *Terminal Agency Coordinator Manual* to serve as a guide for managing Department and other criminal justice agency user access privileges to FCIC; however, the *Manual* did not address the management of elevated levels of FCIC access privileges. The lack of written procedures for managing access increases the risk that access privileges may not be assigned, monitored, or deactivated consistently and in a manner pursuant to management's expectations.

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.

Finding No. 3: Timely Deactivation of Access Privileges

AEIT Rule 71A-1.007(6), Florida Administrative Code, provides that access authorization shall be promptly removed when the user's employment is terminated or access to the information resource is no longer required. Effective access controls include provisions for timely deactivating employee access privileges when employment terminations occur. Prompt action is necessary to ensure that the former employee or others do not misuse the former employee's access privileges.

We compared listings of FCIC and CCH application access privileges as of December 13 and 19, 2011, respectively, to a report of employees who terminated employment between September 1, 2011, and the dates of the access listings and noted that the access privileges of some former employees had not been not timely deactivated. Similar issues were communicated to Department management in connection with our report No. 2004-071. Specifically:

- The FCIC access privileges of 14 of 74 former employees remained active as of December 13, 2011, for periods ranging from 12 to 102 days after termination. The access privileges of the former employees had not been used to perform inquiry or update transactions in FCIC after their termination dates.
- The CCH access privileges of 10 of 78 former employees remained active as of December 19, 2011, for periods ranging from 18 to 108 days after termination. In response to audit inquiry, Department staff provided documentation substantiating that the access privileges of the former employees had not been used to access CCH after their termination dates.

Through additional audit procedures, we found additional former employees whose access privileges had not been timely deactivated. Specifically:

- The FCIC access privileges of two former employees, which were elevated access privileges, remained active as of December 13, 2011, for periods of 137 and 442 days after their termination dates. The access privileges of the former employees had not been used to perform update transactions in FCIC after their termination dates. One of the former employees did perform inquiry transactions subsequent to his termination from the Department. However, these inquiry transactions were within the scope of his new job duties with a local law enforcement organization.
- The CCH application access privileges of four former employees remained active as of December 19, 2011, for periods ranging from 136 to 881 days after termination. In response to audit inquiry, Department staff provided documentation substantiating that the access privileges of the former employees had not been used to access CCH after their termination dates.
- The CCH source library access privileges of one former employee remained active as of January 12, 2012, for 80 days after termination. This former employee also retained CCH application access privileges for 80 days after termination. In response to audit inquiry, Department staff provided documentation substantiating that the access privileges of the former employee had not been used to access CCH after the employee's termination date.
- The FCIC database access privileges of one former employee remained active as of December 9, 2011. The Department could not locate information on the exact termination date of the employee; however, our testing substantiated that the termination date was prior to September 1, 2011. Therefore, the former employee's access privileges had remained active for at least 99 days after the employee's termination date.

Department staff conducted periodic reviews of active CCH users to determine if the users were still active employees of the Department. See Finding No. 4 below for more details of the periodic reviews. As part of their review, Department staff discovered, and on January 20, 2012, deactivated the CCH application access privileges of most of the former employees described above and the CCH source library access privileges of the former employee described above. However, prior reviews of active CCH users were not effective at detecting former employees as noted above. Nevertheless, absent timely deactivation of former employee access privileges, the risk was increased that the access privileges of former employees may be misused by a valid network user or someone with access to an appropriate terminal emulator.

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.

Finding No. 4: Periodic Review of Access Privileges

AEIT Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights periodically. Periodic reviews of user access privileges help ensure that user access privileges remain appropriate. Our audit disclosed that the Department's review of access privileges needed improvement. Specifically:

- The Department did not conduct a comprehensive periodic review of the appropriateness of FCIC application user access privileges. A similar finding regarding review of the appropriateness of FCIC application user access privileges was communicated to Department management in connection with our report No. 2004-071.
- The Department's periodic review of CCH application access privileges, discussed above in Finding No. 3, was only intended to determine whether active CCH users were still employed by the Department. The review did not include an evaluation of the continued appropriateness of current employees' CCH access.
- Department staff did not periodically review logs of changes to FCIC database user access privileges. A similar finding regarding review of the appropriateness of FCIC database user access privileges was communicated to Department management in connection with our report No. 2004-071.

The inappropriate access privileges of current and former employees, described previously in Finding Nos. 1 and 3, indicate a need for the Department to conduct comprehensive periodic reviews of the appropriateness of FCIC and CCH user access privileges and changes thereto. The lack of comprehensive periodic reviews of access privileges and change logs increase the risk that excessive or inappropriate access privileges may not be timely detected or corrected.

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

Finding No. 5: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that 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 No. 2004-071. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate controls in the areas described above, the confidentiality, integrity, and availability of data and IT resources may be compromised.

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.

Finding No. 6: Program Change Management

Effective controls over the modification of application programs help ensure that only authorized, tested, and approved changes are implemented. Monitoring the movement of program changes into the production environment helps to ensure that only authorized program changes were implemented.

Our audit disclosed that FCIC program changes were moved into the production environment manually by system administrators without the use of change control software; therefore, no reporting existed to allow the Department to perform post-implementation reviews to ensure that only authorized FCIC program changes had been moved into the production environment. Although changes to CCH were logged by the system, no post-implementation review was in place to determine if unauthorized changes were made to the system. Under these conditions, the risk was increased that unauthorized changes that impact the proper functioning of FCIC and CCH, should they occur, may not be timely detected. A similar finding with regard to the lack of Department monitoring of the movement of FCIC programs into the production environment was noted in our report No. 2004-071.

Recommendation: The Department should implement a post-implementation review of movement of FCIC and CCH program changes into the production environment to ensure that unauthorized or erroneous changes, should they occur, are timely detected.

Finding No. 7: Use of SSNs

Section 119.071(4)(a), Florida Statutes, provides that all employee SSNs held by the employing agency are confidential and exempt from public inspection. Pursuant to Section 119.071(5)(a)2.a., Florida Statutes, an agency may not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless the agency is specifically authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

The Department collected and used certain employee SSNs in FCIC and CCH. To avoid the possibility of compromising Department information, we are not disclosing in this report the specific details of how the SSN was used. However, we have notified appropriate Department management of this issue.

No specific authorization existed in law for the Department to collect and use certain employee SSNs in FCIC and CCH, and the Department had not established the imperative need to use the SSN for the performance of its duties and responsibilities instead of another number. The use of the SSN was contrary to State law and increased the risk of improper disclosure of SSNs.

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.

Finding No. 8: Disaster Recovery and Backup Controls

AEIT Rule 71A-1.0012(5), Florida Administrative Code, provides that information technology disaster recovery plans shall be tested at least annually. Disaster recovery plans are an important element of effective internal control over IT operations. There are a number of steps that an entity can take to minimize the risk of data loss that may occur from unexpected events. One example is routinely backing up data files and programs. Such actions maintain the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

We noted deficiencies in disaster recovery and backup controls. Specifically:

- The Department had not annually tested the Office of Information Resource Management (IRM) Continuity of Operations Plan (COOP), contrary to requirements specified in the COOP.
- CCH backup tapes were not tested to ensure that backed up data was recoverable.
- Department staff did not maintain a log to track the physical movement of backup tapes, contrary to IRM Procedure 4.100, *Confidential Media Handling Procedure*.

When a disaster recovery plan has not been tested for feasibility or weaknesses, there is an increased risk that restoration of IT operations may be delayed in the event of a disaster. If backup tapes are not readable or cannot be located in the event of a loss of production data, the risk is increased that the Department's ability to timely and completely restore the lost information may be hindered.

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.

PRIOR AUDIT FOLLOW-UP

The Department had partially corrected the findings included in our report No. 2004-071 that were applicable to the scope of this audit.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from September 2011 through February 2012 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.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to FCIC and CCH in achieving management's control objectives in in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2004-171.

The scope of our audit focused on evaluating selected IT controls applicable to FCIC and CCH. The audit included selected general IT controls over logical access to programs, data, and database and application change management. The audit also included data exchange controls between FCIC, CCH, and other significant systems, other selected FCIC and CCH application IT controls, and selected user controls relevant to FCIC and CCH. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from September 2011 through February 2012 and selected Department actions through March 2012.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of FCIC and CCH including the purpose of the application and identification of the users; processing location, hardware, software, and user environments; the application data flow and interfaces; the access authorization process for FCIC and CCH; and the application change management process.
- Evaluated the effectiveness of the procedures for documenting and authorizing user access privileges to FCIC and CCH for Department employees and contractors. Specifically, we reviewed the process for authorizing FCIC access privileges, and we reviewed access authorization documentation for a sample of 25 of 247 active users with CCH application access as of December 19, 2011, who had accessed the system and all 8 active CCH users who had never accessed the system as of December 19, 2011, to determine whether the access authorization forms were on file and whether the forms specified the access privileges being requested.
- Evaluated the appropriateness of application user access privileges granted in FCIC and CCH. Specifically, we reviewed a sample of 20 of 199 active FCIC application user accounts as of December 13, 2011, a sample of 25 of 247 active users account with CCH application access as of December 19, 2011, who had accessed the system and all 8 active CCH users who had never accessed the system as of December 19, 2011, to determine if application user access privileges granted were appropriate.

- Evaluated the appropriateness of logical access privileges to the FCIC development environment, to CCH source libraries, and to move CCH program changes into the production environment. Specifically, we tested 23 active users with FCIC development environment access privileges as of February 14, 2012, and 16 active users with access privileges to CCH source libraries or to move CCH program changes into the production environment as of January 12, 2012. Additionally, we reviewed the FCIC and CCH application access privileges granted to the selected users to determine if the privileges enforced an appropriate separation of incompatible duties.
- Evaluated the appropriateness of logical access privileges to FCIC and CCH system resources (application servers and databases). Specifically, we tested 5 active users with FCIC systems software access privileges as of December 9, 2011, 10 active users with FCIC database access privileges as of December 9, 2011, 12 active users with CCH systems software access privileges as of December 19, 2011, and 5 active users with update access privileges in the CCH database as of December 9, 2011, to determine if systems software and database access privileges granted were appropriate. Additionally, we reviewed the FCIC and CCH application access privileges granted to the selected users to determine if the privileges enforced an appropriate separation of incompatible duties.
- Tested the timeliness of deactivating the FCIC and CCH user access privileges of former Department employees.
- Tested the effectiveness of program change management procedures followed by the Department for FCIC and CCH. Specifically, we reviewed change documentation related to 11 CCH program changes and 4 FCIC program changes completed between September 2, 2011, and November 18, 2011, to determine if change management procedures were effective.
- Observed and evaluated physical and environmental controls of the Department's data center.
- Tested the appropriateness of physical access privileges to the Department's data center. Specifically, we reviewed the privileges of 113 individuals with data center access as of October 31, 2011, to determine if access was appropriate for employee and contractor job functions.
- Evaluated the effectiveness of Department backup procedures.
- Evaluated the effectiveness of patch management procedures followed by the Department.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

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 IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated October 19, 2012, the Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

FDLE

Florida Department of Law Enforcement

Gerald M. Bailey
Commissioner

Office of Executive Director
Post Office Box 1489
Tallahassee, Florida 32302-1489
(850) 410-7001
www.fdle.state.fl.us

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

October 19, 2012

Mr. David Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

We are in receipt of the Preliminary and Tentative Findings Report on the

Information Technology Operational Audit
Department of Law Enforcement
Florida Crime Information Center (FCIC) and
Computerized Criminal History System (CCH).

Please see the Department's attached response to the report. If you require further information, please contact Inspector General Al Dennis at 410-7000.

Sincerely,

Mark A. Zadra, Assistant Commissioner for

Gerald M. Bailey
Commissioner

Attachment

GMB/AL/lht

Service • Integrity • Respect • Quality

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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 FCIC and 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.

FDLE Response:

FDLE concurs with the finding.

When the Department became aware of user accounts with inappropriate access privileges during the audit exit conference on September 21, 2012, it immediately began modifying or deactivating such accounts as could immediately be identified. Our response to finding 2 of this audit further details how we will address this issue in the future.

A CCH application programming flaw related to access privileges that was identified during the audit period was patched on September 18, 2012. We wish to remark that a review of application logs proved that the flaw had never been exploited.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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.

FDLE Response:

FDLE concurs with the finding that the Department should maintain complete documentation of management authorization including authorized signature for user access that specifies user privilege assignment. The agency also concurs with the recommendation to maintain documentation for elevated levels of access to FCIC.

Terminal Agency Coordinators (TACs) serve as FCIC access administrator for the agency; at both FDLE and local agencies. The pending revision to our internal agency policy regarding Application Access Administrators will further clarify the procedures for management of FDLE member access.

The Department will develop procedures that address access to CCH and periodic reviews of user access privileges for FCIC and CCH.

FDLE plans to have the revised policy and new procedures in place by July 2013.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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.

FDLE Response:

The Department concurs with the finding.

Prior to the Auditor General's review, FDLE had begun developing policy and procedures for Application Access Administration (AAA) which encompasses not only the FCIC and CCH, but all major information systems in the agency. As a result of the agency's AAA policy development process, Criminal Justice Information Services deactivated CCH user accounts that were no longer being used and as part of the revised procedure, agency Application Access Administrators review Employee Status Reports (distributed by FDLE's Office of Resources) for those affected by personnel actions and modify permissions and/or terminate access to the CCH system as appropriate.

The Department reiterates that CJIS Certification is valid for the user for a designated period of time, and although required for FCIC access, is maintained separately from FCIC application access. FCIC is a statewide system, and FDLE user access to FCIC is managed through individual agency application software, and not directly through the FCIC database/message switch. CJIS Certification for individual users will remain intact until such time as the certification expires. However, FDLE concurs with the recommendation that usercodes should be deactivated upon termination from the agency and will work toward formalizing a procedure.

FDLE plans to have procedures in place by July 2013.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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.

FDLE Response:

The Department concurs with the finding.

Prior to the Auditor General review, FDLE had begun the process of developing policy and procedures for Application Access Administration (AAA) which encompasses not only the FCIC and CCH systems, but all major information systems in the agency. As a result of the agency's AAA policy revision, which also occurred during the course of the Auditor General review, Criminal Justice Information Services began deactivating CCH user accounts that were no longer applicable. The draft agency policy addressing Application Access Administration is currently under review. Application Access Administrators will review internal Employee Status Reports to ensure timely modifications or removal of access is processed. In addition, the agency will complete periodic comprehensive reviews for appropriateness of access to FCIC and CCH at least every six months.

FDLE plans to have the agency policy and supporting procedures in place by July 2013.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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.

FDLE Response:

FDLE concurs with the finding.

The recommendation has been designated a top priority and the Department is already taking affirmative action to address the deficiencies identified in this finding. Due to the sensitive nature of these findings and recommendation, we will not disclose specific details of mitigation activities in this response.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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 was noted in our report Number 2004-071.

Recommendation:

The Department should implement a post-implementation review of 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.

FDLE Response

FDLE concurs with the finding.

The Department adheres to an established and well-documented change control process for moving programming changes, including those for FCIC and CCH, from development to production environments. Before a programming change is placed into production, it must pass at least two formal reviews with involvement from the program customer, development and production technical teams, the information security manager, end-user support teams, and senior management.

However, the Department recognizes that this process can be improved through the use of automated tools.

The Department will investigate the feasibility and cost-effectiveness of implementing an automated tool for managing FCIC programming changes to augment the existing change control process. No date is being set for implementing these changes at this time as research is needed to document specific requirements, identify products, and budget for proposed changes.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 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.

FDLE Response:

Because this finding is confidential in nature, the Department acknowledges the recommendation and will take it under advisement for future initiatives.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Law Enforcement
Response to the Auditor General
Preliminary and Tentative Audit Findings
Information Technology Operational Audit
Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) Systems

Finding Number 8: Disaster Recovery and Backup Controls

The Department 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.

FDLE Response:

FDLE concurs with the finding.

The Department's IRM COOP has been designated for immediate review/revision with the objective of formulating a COOP test plan. Execution of the COOP test plan will be included as a component of the Department's 2013-2014 Information Security Strategic Plan. In addition, IRM will reevaluate the enforcement of its internal procedure governing backup tape handling and will document the requirements and procedure for testing of FCIC and CCH backup tape integrity.