AUDITOR GENERAL

DAVID W. MARTIN, CPA

DEPARTMENT OF LEGAL AFFAIRS
LOTUS NOTES APPLICATIONS

Information Technology Audit

SUMMARY

The Department of Legal Affairs (Department) uses Lotus Notes software to develop, maintain, and operate over 300 custom applications to perform its day-to-day functions. The custom applications include functionality to support legal case management, victims' claims processing, complaint and correspondence tracking, administrative and financial systems, workflow and collaboration, Web content management, and Web-based consumer services.

Our audit focused on evaluating the Department's use of Lotus Notes to implement selected systems development and modification, data security, and data integrity controls over the custom Lotus Notes applications during the period April 2008 through July 2008. In addition, we determined the status of corrective actions regarding selected prior audit findings disclosed in audit report No. 02-023.

The results of our audit are summarized below:

Finding No. 1: Aspects of the Department's Lotus Notes systems development software, and the Department's configuration thereof, limited the Department's deployment of appropriate systems development controls.

Finding No. 2: The Department's policies and procedures did not provide for certain systems development controls included in industry best practices.

Finding No. 3: Some instances existed where the Department lacked documentation of the authorization and testing of program changes, the approval of program changes for implementation, and the names of employees who moved program changes into production.

Finding No. 4: Some instances existed of excessive and inappropriate access privileges to Lotus Notes applications and data.

Finding No. 5: In addition to the matters discussed in Finding No. 4, certain Department security controls related to Lotus Notes and the supporting network environment needed improvement. We have not disclosed specific details of these issues in this report to avoid the possibility of compromising the Department's data and IT resources.

BACKGROUND

The Department of Legal Affairs, headed by the Attorney General, is responsible for providing legal services required by any Department within the State of Florida, unless otherwise provided by law. The Department's various statutory responsibilities for the conduct of day-to-day business include, but are not limited to, programs to assist victims of crimes, enforcement of State consumer protection and antitrust laws, as well as civil prosecution of criminal racketeering.

The Department uses Lotus Notes software to support its business units in carrying out assigned functions. Lotus Notes is a groupware product that allows people to share information and work together on projects. The Application Development staff within the Division of Information Technology (IT) develops and maintains custom Lotus Notes applications utilizing an iterative development process known as rapid application development (RAD). RAD involves building the application in iterations or

increments, with feedback from the project owner occurring after each increment to facilitate any necessary adjustment of project plans and software development.

Finding No. 1: Development Software

Development software is used to control the development and modification of programs. Typical development software provides the capability to produce logs of all program changes to detect unauthorized changes from being made inadvertently or deliberately. The software also often controls access to programs to ensure that multiple programmers are prevented from concurrently changing the same program and enforces separation of duties by precluding developers from having access to production. Lotus Notes as utilized by the Department included development software that was used to manage the development and modification of application programs.

Our audit disclosed aspects of the Department's Lotus Notes development software and the configuration of the software that limited the Department's deployment of appropriate systems development controls. Specifically:

- The software did not provide the capability to retain historical logs of program changes other than the most recent change. This increases the risk that unauthorized changes could be made and not be timely detected.
- The software included a design lock feature that, if activated, would preclude concurrent development of the same program. However, the Department had not activated the design lock feature. Under these conditions, the risk is increased that program changes made by one developer could be overwritten by another developer before being moved to production.
- The software did not provide the ability to control developers' access to data separately from application programs. Lotus Notes is designed in such a manner that programs and data are stored together in the same structure (a Notes Storage Facility). As a result, the Department was prohibited from restricting developers from accessing production data if the developers needed access to production programs, and developers had the ability to view, modify, and delete production data. Under these conditions, the risk of unauthorized disclosure, modification, or destruction of Department data is increased.

Recommendation: The Department should develop or acquire the capability to retain and monitor logs of program changes. Additionally, the Department should activate the design lock feature for Lotus Notes application programs and enforce a separation of duties such that developers do not have access to production data.

Finding No. 2: Systems Development Policies and Procedures

Written policies and procedures serve to communicate management's expectations for how functions and activities are to be performed and controlled. In the IT environment, systems development policies and procedures document management's expectations for the development and modification of application systems.

As a part of our audit, we compared the Department's Automated Information Systems Change Management Procedure (Procedure) to industry systems development best practices. Our comparison disclosed that the Procedure did not provide for certain systems development controls included in industry best practices. Specifically, the Procedure lacked provisions for:

- As part of the RAD process, application development staff and project owners to identify risks and discuss strategies for control auditability, security, and availability of the Lotus Notes applications and document the discussions.
- Documentation of the approval of iterations or increments of program development or changes, including the final movement of a program into production.
- Documentation of project owner approval of minimal ad hoc changes prior to the changes being moved into production.

- Documentation of approval of emergency changes by the application owner and IT management after the change has been moved into production.
- An appropriate separation of duties between the development of programs and the movement of programs into production. The Procedure stated that the project coordinator was the lead developer on the project and responsible for moving programs into production.

Absent the above-listed provisions, the risk is increased that program changes will not be appropriately authorized, developed, tested, and approved, jeopardizing the ongoing integrity of application systems and data.

We also noted that the Procedure required that all actions taken or modifications be documented. However, Department staff stated, in response to audit inquiry, that not all ad hoc changes were documented. The absence of a complete record of development actions and modifications could hinder the accuracy and efficiency of future program modifications.

Additionally, our audit disclosed that the Department did not have a policy for the classification of data according to risk and importance to support decisions regarding the appropriate level of data protection to be employed during systems development and change activities. The absence of data classification could hinder Department efforts to identify, classify, and mitigate risks associated with its application systems and data.

Recommendation: The Department should update the Procedure to include provisions as described above to ensure appropriate planning, development, approval, and implementation of application systems and modifications thereto. In addition, a complete record of all development and modification activities should be maintained to assist in the ongoing management of system changes. Furthermore, the Department should establish a data classification policy to provide for the categorization of data according to risk and importance to the Department's mission to aid in risk management decisions.

Finding No. 3: Lotus Notes Application Program Change Controls

Effective controls over changes to application programs are intended to ensure that only authorized and properly functioning program changes are implemented. Application program change controls include procedures to ensure that all program changes are properly authorized, tested, approved for implementation, and implemented by someone other than the developer who programmed the change.

As previously discussed in Finding No. 1 above, the Lotus Notes development software did not provide the capability to log and track all program changes. Notwithstanding the limitations of obtaining a complete list of program changes, we tested 30 program changes from ten selected Lotus Notes applications, as manually documented in the Department's Lotus Notes database registry, and noted the following:

- For 6 changes, no documentation of program change authorization.
- For 20 changes, no documentation that the program change was tested to ensure the requested functionality was achieved.
- For 27 changes, no documentation of approval by the project owner and IT management for the program changes to be moved into production.
- No documentation to demonstrate who moved program changes into production.

Under these conditions, the risk is increased that unauthorized or erroneous program changes will be moved into production without timely detection.

Recommendation: The Department should enforce appropriate program change controls that include documentation of authorization, testing, and approval of all Lotus Notes application program changes and the movement of program changes into production.

Finding No. 4:
Appropriateness of Access Privileges

Access controls include the establishment of access accounts with privileges that restrict users to only those system functions necessary to perform their assigned duties, and the establishment of individual system access accounts for each user to ensure accountability. Properly configured access privileges help minimize the risk of unauthorized system actions.

Our testing of IT employee access privileges to ten selected Lotus Notes applications and the Department's Lotus servers disclosed instances of excessive or inappropriate access privileges. Specifically:

- Ten IT employees were granted administrative privileges to Lotus servers, providing capabilities to create and delete databases, which are the basis for Lotus applications. The administrative privileges also provided capabilities to modify access control lists. Additionally, we noted instances where Application Development employees used administrative privileges to modify production data in response to requests by authorized personnel. Inappropriate and excessive access privileges, as well as developer access to production data, increases the risk of unauthorized or erroneous disclosure, modification, or destruction of data and IT resources.
- Department Lotus Notes applications utilized a system account to ensure that executable instructions for the applications had permissions to run on the Lotus Notes servers. All Application Development employees knew the credentials to the system account and granted the applications they developed the required system account access privileges. However, in some instances, Application Development employees also utilized the system account privileges to update production programs. The use of the system account by more than one individual limited the Department's ability to establish accountability for Application Development employees making changes to production systems.

Recommendation: The Department should ensure that the access privileges of employees are commensurate with their job duties and best practices. Additionally, the Department should limit and monitor the use of the system account to reduce the risk of unauthorized system actions and to promote accountability.

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 certain Department security controls related to Lotus Notes servers and the surrounding IT infrastructure that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should implement the appropriate security controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

PRIOR AUDIT FINDINGS

Finding No. 4 above included an issue repeated from our audit report No. 02-023. The other IT deficiency noted in the prior audit that was within the scope of this audit has been corrected.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to evaluate the Department's use of Lotus Notes to implement selected systems development and modification, data security, and data integrity controls over the custom Lotus Notes applications and to determine whether management has corrected, or was in the process of

correcting, selected prior audit findings disclosed in audit report No. 02-023.

The scope of our audit focused on evaluating selected IT controls applicable to the Department related to its use of Lotus Notes for application development in its operations during the period April 2008 through July 2008.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the Department's use of Lotus Notes for systems development and modification.
- Observed, documented, and tested key processes and procedures related to the Department's systems development and modification activities.
- Evaluated the Department's Lotus Notes systems development software and configuration, policies and procedures related to systems development, network and Lotus Notes server logical access management, and techniques to safeguard data.

We conducted this IT audit in accordance with applicable 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.

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 audit.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated October 7, 2008, Department management provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **APPENDIX A**.

This audit was conducted by Geoffrey Adams, CISA, and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, via e-mail at 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.myflorida.com/audgen/); by telephone (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

APPENDIX A

MANAGEMENT RESPONSE

BILL McCOLLUM
ATTORNEY GENERAL
STATE OF FLORIDA

OFFICE OF THE ATTORNEY GENERAL

Bill Stewart
Deputy Chief of Staff

The Capitol, PL 01
Tallahassee FL 32399-1050
Telephone (850) 245-0184
Fax (850) 487-2564

October 7, 2008

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

Dear Mr. Martin:

As required by Section 11.45(4)(d), Florida Statutes, the Department's response to the preliminary and tentative findings and recommendations related to your Information Technology Audit of the Department of Legal Affairs, Lotus Notes Applications, for the period April 2008 through July 2008 is attached.

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact our Inspector General James D. Varnado, at 414-3456.

Sincerely,

Bill Stewart

WDS:bls
Attachment

Response to Preliminary and Tentative Audit Findings
Department of Legal Affairs
Lotus Notes Applications
For the Period April 2008 through July 2008

Finding No. 1: Aspects of the Department's Lotus Notes systems development software, and the Department's configuration thereof, limited the Department's deployment of appropriate system development controls.

Recommendation: The Department should develop or acquire the capability to retain and monitor logs or program changes. Additionally, the Department should activate the design lock feature for Lotus Notes application programs and enforce a separation of duties such that developers do not have access to production data.

Response: Development or procurement of any additional software will be considered, but will be constrained by current budget and resource limitations. The Department will review and modify the Automated Information Systems Change Management Procedure to address the following:

1. Clarification of roles and responsibilities for development staff and business project owners, throughout the entire system life cycle;
2. Centralization of appropriate documentation of the authorization, testing, production implementation and acceptance of changes and versions;
3. System, data and request classification as to confidentiality, mission criticality, urgency and fraud risk;
4. Revision and expansion of procedures, based upon above-mentioned roles, responsibilities, and classification, to appropriately address separation of duties, concurrent development, logging of program changes, and the use of the Lotus Notes design lock feature, as feasible within resource constraints.

Finding No. 2: The Department's policies and procedures did not provide for certain systems development controls included in industry best practices.

Recommendation: The Department should update the Procedure to include provisions as described above to ensure appropriate planning, development, approval, and implementation of application systems and modifications thereto. In addition, a complete record of all development and modification activities should be maintained to assist in the ongoing management of system changes. Furthermore, the Department should establish a data classification policy to provide for the categorization of data according to risk and importance to the Department's mission to aid in risk management decisions.

Response: We believe the action items detailed in Finding No. 1 appropriately resolve these issues.

Finding No. 3: Some instances existed where the Department lacked documentation of the authorization and testing of program changes, the approval of program changes for implementation, and the names of employees who moved program changes into production.

Recommendation: The Department should enforce appropriate program change controls that include documentation of authorization, testing, and approval of all Lotus Notes application program changes and the movement of program changes into production.

Response: We believe the action items detailed in Finding No. 1 appropriately resolve these issues.

Finding No. 4: Some instances existed of excessive and inappropriate access privileges to Lotus Notes applications and data.

Recommendation: The Department should ensure that the access privileges of employees are commensurate with their job duties and best practices. Additionally, the Department should limit and monitor the use of the system account to reduce the risk of unauthorized system actions and to promote accountability.

Response: The Department will reassess the appropriateness of current access privileges, and, where feasible within resource constraints, support requirements and assigned job duties, will further restrict employee access privileges.

Finding No. 5: In addition to the matters discussed in Finding No. 4, certain Department security controls related to Lotus Notes and the supporting network environment needed improvement. We have not disclosed specific details of these issues in this report to avoid the possibility of compromising the Department's data and IT resources.

Recommendation: The Department should implement the appropriate security controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response: The Department will assess current security controls and implement procedural and technical changes to strengthen these controls as feasible.