



Fairfax County Internal Audit Office

Fairfax County Police Department
I/LEADS Application Audit
Final Report

January 2013

"promoting efficient & effective local government"

NOTE: Certain sensitive and confidential police operational related information has been omitted from general disclosure. This information, if disclosed, would subject the Police Department to potential program risks.

Executive Summary

The Fairfax County Police Department (FCPD) uses I/LEADS, a comprehensive records management software package from Intergraph, Inc., to provide integrated, comprehensive management and processing of the many types of data used by the department such as citation, accident, arrest, and incident data. It tracks FCPD's compliance with the many federal and state requirements and regulations, and interfaces with systems used by other divisions of the criminal justice system, such as the Fairfax County Sheriff, the Commonwealth of Virginia courts, and with National Capital Region Law Enforcement Information Exchange (NCR LInX).

System controls were adequate and information was entered into the I/LEADS system accurately and completely. The FCPD system administrator staff demonstrated a strong understanding of these controls. Data and system files were backed up on a daily basis with a copy of the backups being stored offsite as well by the Department of Information Technology (DIT). Internal controls concerning the physical security of the servers were strong. Finally, the system administration functions were adequately controlled except as stated below. We noted an area where these controls could be strengthened in regard to the separation of duties and recordkeeping.

- FCPD did not have written procedures for the addition and deactivation of users in I/LEADS and there was no record kept of the authorizations for these changes in access.

Scope and Objectives

This audit was performed as part of our fiscal year 2012 Annual Audit Plan and was conducted 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. This audit covered the period of January 1, 2011, through January 1, 2012, and our audit objectives were to determine that:

- System controls for the application were in place and adequate.
- System input, processing, security, reporting, and printing capabilities were secure and well documented.
- Data safeguards, application access, transaction audit trails, backup and recovery of data and separation of duties were well monitored.

There were eight interfaces between I/LEADS and other applications at the time of our audit. This audit focused on I/LEADS data up to the point of interface with other systems. We verified that controls were in place to assure the clean transfer of I/LEADS data.

Methodology

Our audit approach included a review and analysis of internal controls over the I/LEADS application data input, processing, and output. We interviewed appropriate employees to understand the application process, observed employees' work functions; and performed substantive testwork to determine if controls were in place to prevent data from unauthorized access and modification.

Our audit did not examine the Property/Evidence module of I/LEADS. The property/evidence application previously used by the Police Department (BEAST) was audited in FY 2008. Currently the department is using both BEAST and I/LEADS in their property room. All new property and evidence received is entered into I/LEADS and existing property and evidence records are maintained in BEAST. Because of this situation and the fact that this was a large area of processing within the police department, the decision was made to audit this module separately at a later date.

Findings, Recommendations, and Management Response

Userid Maintenance

There were no written procedures for granting or changing user access to I/LEADS and no record was kept of the business justification for or approval of these changes. Per discussions with the system administrator, changes to I/LEADS access required an e-mail sent to the system administrators. The system administrators verified that training had been completed for new users and then added them to the appropriate group in I/LEADS. When there was a need for the deactivation of a user, the personnel division or internal affairs division of the Police Department sent an e-mail to the system administrators, who then deactivated the userid. The e-mails were not maintained on file.

Recommendation: Written procedures should be developed for the process of adding, changing, and deactivating a userid in I/LEADS. Records should be maintained to include the e-mail authorization including a business justification for each addition/deactivation. A report or online screen should show for a given time period all additions/deletions of userids. The manager of the central records division should regularly review this list and investigate unusual activity.

Management Response: A change in a user profile will be supported by either an e-mail request or an online Police Employment Action Request (EAR) form from the Commander of the unit which will include the business reason for the change. A copy of the email or EAR form will be kept in an online folder. A before and after

version of the user profile will be saved as a PDF in a shared folder. The Manager of Central Records will review this folder on a set schedule. A written policy will be sent out to all commanders defining this process for adding, changing, and deactivating userids. The anticipated completion date is December 17, 2012.