Richmond City Council

The Voice of the People. *Richmond, Virginia*

OFFICE OF THE CITY AUDITOR

REPORT # 2012-10
AUDIT
Of the

Richmond Police Department
Police Records Management System (PISTOL)

12 Months ended December 31, 2011

OFFICIAL GOVERNMENT REPORT

Richmond City Council
OFFICE OF THE CITY AUDITOR
900 East Broad Street, 8th Floor
Richmond, Virginia 23219

804.646.5616 (tel); 804 646.2230 (fax)

Committed to increasing government efficiency, effectiveness, and accountability on behalf of the Citizens of Richmond.

TABLE OF CONTENTS

Richmond City Council

The Voice of the People Richmond, Virginia

Office of the City Auditor

Umesh Dalal, CPA, CIA, CIG
Richmond City Auditor

Executive Summary

June 26, 2012

The Honorable Members of the Richmond City Council
The Honorable Mayor Dwight C. Jones

Subject: Police Department – PISTOL Records Management System

The City Auditor’s Office has completed an audit of the Police Department’s PISTOL Records Management System (PISTOL). PISTOL Records Management System (RMS) is a critical application used to collect, store, and provide access to all of the information gathered by law enforcement personnel.

For the purpose of this report, the auditors classified deficiencies observed based on the following criteria:

***High Risk* -** Represents major deficiency resulting in significant level of risk. Immediate management attention is required.

Medium Risk- Represents control weakness resulting in an unacceptable level of risk that if left uncorrected may deteriorate to a high risk condition.

***Low Risk* -** Control weakness exists but the resulting exposure is not significant.

Based on the results and findings of the audit methodology employed, auditors concluded that internal controls relevant to PISTOL RMS are adequate and functioning effectively. However, the auditor noted some control deficiencies in our testing. Management attention is required to expediently address all the discrepancies labeled as high and medium risk in the accompanying report.

The City Auditor’s Office appreciates the cooperation of the Police Department’s staff. Please contact me for questions and comments on this report.

Sincerely,

Umesh Dalal

Umesh Dalal, CPA, CIA, CIG
City Auditor

cc: Mr. Byron C. Marshall, CAO
The Richmond City Audit Committee
Chief Bryan Norwood

#	*COMPREHENSIVE LIST OF RECOMMENDATIONS*	*PAGE*
1	Perform tape backups of the PISTOL RMS application and database on a daily basis.	4
2	The Police Department needs to invest in failover capability for the PISTOL RMS.	4
3	Remove or disable the default System Administrator account if it does not affect the system functionality.	4
4	Restrict the users in “ALLRIGHTS” group to PISTOL RMS Administrator and backups.	5
5	Ensure that MFR functions in the Police cars even if the connection between DEC and the City Hall is lost.	5
6	Turn on password expiration and complexity settings for the PISTOL RMS application.	6
7	Upgrade the PISTOL SQL database to SQL2008.	6
8	Develop performance indicators for • Average time for resolution of major and minor application issues; • Number of incidents reopened; and • Percentage of incidents not resolved within the agreed upon timelines.	7
9	Establish a formal written security policy outlining the approval requirements for granting, modifying and removing access to PISTOL using least privilege principle (minimum level of access).	7
10	Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for PISTOL application users.	7
11	Develop policies and procedures for managing changes, including minor application changes, major application changes and software releases. This should include procedures for testing and receiving proper authorization and are supported by a change request document.	8
12	Document the results of the periodic review of user access to PISTOL and actions taken to address the issues, if any.	8
13	Evaluate the cost-benefit of purchasing the E-Ticketing module. If the cost is beneficial, purchase and implement Pistol E-Ticketing module.	8

City of Richmond Audit Report
Richmond Police Department
Police Records Management System (PISTOL)
12 Months ended December 31, 2011

Introduction

The City Auditor’s Office has completed an audit of the Police Department’s PISTOL Records Management System (PISTOL). This audit covers the 12-month period ended December 31, 2011. The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and Control Objectives for Information and related Technology (COBIT) guidelines issued by the Information Systems Audit and Control Association (ISACA). Those standards provide a reasonable basis for the conclusions regarding the internal control structure over PISTOL and the recommendations presented.

Audit Objectives and Methodology

- Determine whether adequate IT general controls for access to programs and data, program changes and computer operations have been established by management;
- Verify compliance with applicable laws and regulations; and
- Determine if PISTOL processing is complete and accurate and supports business operations.

Auditors employed the following methodologies to complete this audit:

- Interviewed relevant personnel;
- Reviewed policies and procedures;
- Reviewed system data, configurations, and reports; and
- Conducted other tests, as deemed necessary.

The management of the City of Richmond is responsible for maintaining relevant records and maintaining a system of internal accounting and management controls. In fulfilling this responsibility, management is required to assess the expected benefits and related costs of the control procedures.

Background

PISTOL Records Management System (RMS) is a critical application used to collect, store, and provide access to all of the information gathered by law enforcement personnel. PISTOL RMS records and stores all information gathered during the course of investigating an incident. This information enables the Police Department to protect the citizens and helps them in the day to day Police activities. It also promotes the safety of the officers by providing real time information.

The key modules of the PISTOL RMS include, but are not limited to:

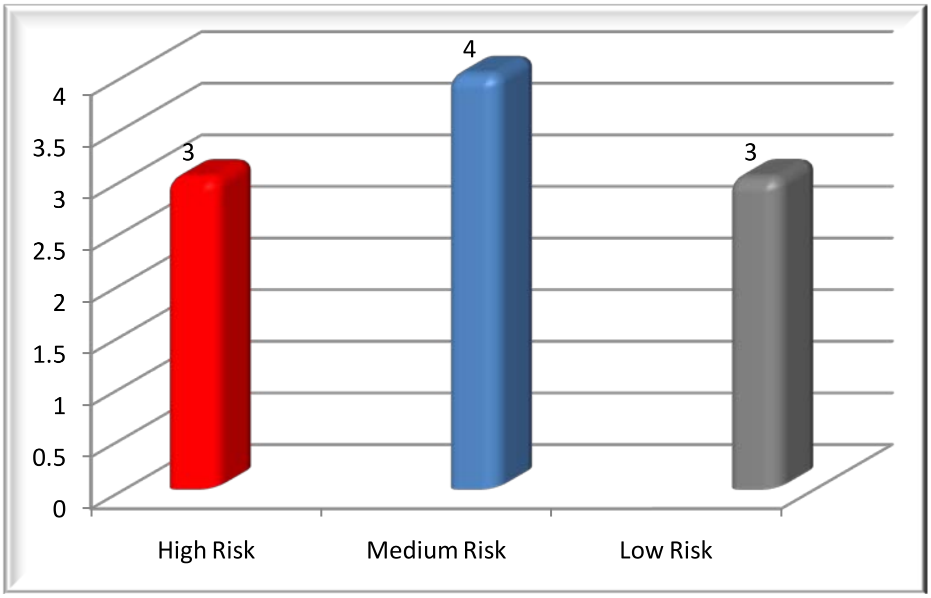
- ***Incident:*** Allows users to enter and maintain Incident reports taken by the agency and used for State Incident Based Reporting (IBR)/Uniform Crime Reporting (UCR).
- ***Warrant:*** Allows users to manage warrants efficiently within the agency. Many features are supported, including linking a warrant to an Incident/Investigation case and warrant tracking.
- ***Arrest:*** Allows users to enter and maintain arrests by agency.
- ***Traffic Summons:*** Allows users to enter and maintain Citations/Summons issued by the agency.
- ***Accident:*** Allows users to gather and print all of the information required on accident reports.

PISTOL RMS is administered by the Technology Division within the Police Department. The Division is responsible for the day-to-day management of the system, including application administration, application security, computer operations, and end-user support. The Department of Information Technology team is responsible for maintaining the support systems (Servers and Database).

PISTOL RMS is a critical system to the Police Department since it is used for the daily operations and holds the data used for protecting citizens and providing timely information for the safety of the officers. PISTOL RMS data is also used for management reporting and State Incident Based Reporting.

Summary of Findings

The following is a graphical presentation of the level of risk involved for the identified control weaknesses:



Legend:

***High Risk* -** Represents major deficiency resulting in significant level of risk. Immediate management attention is required.

***Medium Risk*-** Represents control weakness resulting in an unacceptable level of risk that if left uncorrected may deteriorate to a high risk condition.

***Low Risk* -** Control weakness exists but the resulting exposure is not significant.

Overall Conclusion

This audit was conducted to evaluate the design and effectiveness of selected internal controls relevant to the PISTOL RMS application. Based on the results and findings of the audit methodology employed, auditors concluded that internal controls relevant to PISTOL RMS are adequate and functioning effectively. However, the auditor noted some control deficiencies in our testing. Management attention is required to expediently address all the discrepancies labeled as high and medium risk.

The following table provides a summary of the findings identified during the audit. The findings are classified into three categories (high, medium and low) based on financial and security risk exposure:

What did the auditors find?	What is the risk?	Recommendation (How to mitigate the risk?)
Lack of daily PISTOL RMS application and database backups: PISTOL RMS application and database tape backups are not performed except for Tuesdays. The Federal Information System Controls Audit Manual (FISCAM) recommends routinely copying data files and software and securely storing these files at a remote location to mitigate service interruptions.	**Risk Level: High** Without proper application and database tape backups, the Police Department runs the risk of permanently losing the application and data files if the system suffers interruptions. In case of a major disaster, the Police Department will not be able to recover the critical case files required for police operations.	1. Perform tape backups of the PISTOL RMS application and database on a daily basis.
Lack of PISTOL RMS failover capability: Currently PISTOL RMS does not have a failover capability. As per the management, the Computer Aided Dispatch (CAD) system has the failover capability to support 911 calls. In the event of telephone service failure, all calls will be transferred to Henrico County. Should it become necessary to evacuate the communications center, DEC personnel and supervisors will report to Henrico County.	**Risk Level: High** Lack of failover could halt or delay police processes due to lack of PISTOL RMS availability and also have the potential to endanger the lives of officers.	2. The Police Department needs to invest in failover capability for the PISTOL RMS.
Excessive administrator access	**Risk Level: High**	3. Remove or disable

What did the auditors find?	What is the risk?	Recommendation (How to mitigate the risk?)
accounts: Administrator privileges provide sensitive access to PISTOL RMS modules and data. Administrator privileges allow users to add or delete other users, assign users to groups, and define rights for security groups. There are six (6) user accounts belonging to the "ALLRIGHTS" Administrator group that provide them with administrator access privileges to PISTOL RMS application. Also, there is a generic account (System Administrator) with no accountability of ownership. As recommended by COBIT, user access should be based on a "least privilege" and "need-to-know" basis. This ensures users have adequate access that is specifically and legitimately required for performing their assigned job duties.	Without limiting administrative access to the appropriate individuals, there is a greater chance of unauthorized: a. Changes to system software, data, modules, or applications. b. Access to system resources. c. Changes to system functionality by bypassing segregation of duties, edit checks, creating fictitious accounts and processing payments, etc. The above situation is undesirable and can be misused; if misused, some or all system processes could be affected, making the system unreliable or unavailable. Therefore, the risk associated with this finding should be addressed immediately.	the default System Administrator account if it does not affect the system functionality. 4. Restrict the users in "ALLRIGHTS" group to PISTOL RMS Administrator and backups.
Mobile Field Reporting (MFR)will not talk to PISTOL if the network is down: Police will be able to use MFR functions in vehicles but the information will not be send over to the PISTOL RMS if the network connection between the City and the Division of Emergency Communications (DEC) is lost.	**Risk Level:** **Medium** Lack of failover could halt or delay police processes due to lack of System availability.	5. Ensure that MFR functions in the Police cars even if the connection between DEC and the City Hall is lost.

What did the auditors find?	What is the risk?	Recommendation (How to mitigate the risk?)
Inadequate password requirements: For PISTOL RMS, strong password settings are not enabled such as requiring: • the passwords to expire after certain number of days to force users to change passwords periodically. • password complexity (requiring passwords to have uppercase and lowercase characters, special characters, etc.) PISTOL RMS is supported by a SQL 2000 database. Password requirements cannot be configured on this version of SQL. Upgrading to the latest version of SQL 2008 will allow the above functionality. COBIT best practices requires control over the IT process of ensuring systems security to safeguard information against unauthorized use, disclosure, modification, damage or loss.	**Risk Level:** **Medium** Without strong passwords, there is a greater potential for: a. Gaining unauthorized access to the system by guessing the passwords and masquerading as other users. b. Gaining access to sensitive data and copying them for personal gain or use by another company. c. Making unauthorized changes to the system software, modules, or applications. The auditor deemed the risk to be medium as users need to sign on to the City's network prior to accessing the PISTOL RMS application. Also the Pistol RMS application has strong audit logging capability to track changes made by the application users. There is a greater threat with internal users misusing the system weak passwords. Secure passwords are probably more critical for protection from internal threats than external threats.	6. Turn on password expiration and complexity settings for the PISTOL RMS application. 7. Upgrade the PISTOL SQL database to SQL2008.
System auditing for failed login attempt were not enabled:	**Risk Level:**	N/A; Management has already turned on the

What did the auditors find?	What is the risk?	Recommendation (How to mitigate the risk?)
System auditing after three failed attempts was not enabled during the audit period. Therefore, the details of the failed attempts to login to the application were not captured.	**Medium** Without a logging and monitoring function, early prevention and/or detection, and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed cannot be performed.	system auditing for failed login attempts for the PISTOL system.
Lack of performance measures Key performance indicators are not developed for • Average time for resolution of major and minor application issues • Number of incidents reopened • Percentage of incidents not resolved within the agreed upon timelines.	**Risk Level:** **Medium** Without performance indicators management cannot access, review, analyze business strategies, capabilities and technology and act upon to deliver positive results towards improving performance.	8. Develop performance indicators for • Average time for resolution of major and minor application issues; • Number of incidents reopened; and • Percentage of incidents not resolved within the agreed upon timelines.
Lack of security policies and procedures: Management has not documented and communicated security policies and procedures that provide the overall framework for managing PISTOL security and guidelines for enforcing information security controls. The security policies and procedures should include coverage of the following areas: 1. The process and associated roles and responsibilities for requesting	**Risk Level: Low** When user account management and authentication policies for granting, modifying, removing or authenticating access to the PISTOL are not set forth and therefore not communicated to all stake holders, there is a potential for allowing users to have inappropriate access to information, applications, and infrastructure that are not required for their job responsibilities.	9. Establish a formal written security policy outlining the approval requirements for granting, modifying and removing access to PISTOL using least privilege principle (minimum level of access). 10. Develop policies and procedures requiring the use of logical access authentication

What did the auditors find?	What is the risk?	Recommendation (How to mitigate the risk?)
and approving user access to PISTOL. 2. The process and associated roles and responsibilities for terminating access to PISTOL and general support systems. 3. The process and associated roles and responsibilities to review user access rights to the PISTOL and general support systems. The review should include: a. A log of any exceptions noted; and b. The final disposition of exceptions; 4. A security policy requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all users of PISTOL. 5. The process and associated roles for requesting, tracking, approving and testing minor application fixes, major application fixes and product releases.	Lack of policies and procedures for managing PISTOL changes could lead to unauthorized changes or inadequately tested changes to be deployed to production.	controls through the assignment of unique user IDs and strong passwords for PISTOL application users. 11. Develop policies and procedures for managing changes, including minor application changes, major application changes and software releases. This should include procedures for testing and receiving proper authorization and are supported by a change request document.
User access needs to be monitored: Periodic review of the defined user groups and user access to PISTOL is performed but not documented. This is a prudent practice to assure security of data and information.	**Risk Level: Low** Failure to perform periodic reviews increases the risk that individuals have unauthorized access to the system.	12. Document the results of the periodic review of user access to PISTOL and actions taken to address the issues, if any.
E-Ticketing module not purchased: Pistol e-ticketing module allows the officers to enter summons on their Mobile Data Computers, print the e-	**Risk Level: Low** Manual process increases the likelihood of data inaccuracies and inefficiencies.	13. Evaluate the cost-benefit of purchasing the E-Ticketing module. If the cost is beneficial, purchase

What did the auditors find?	What is the risk?	Recommendation (How to mitigate the risk?)
ticket for the citizen, and then transmit the summons to Pistol for electronic submission to the courts. This module was not purchased and the information has to be manually keyed into the system.		and implement Pistol E-Ticketing module.

MANAGEMENT RESPONSE FORM

RICHMOND POLICE DEPARTMENT

#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
1	***Perform tape backups of the PISTOL RMS application and database on a daily basis.***	Y	
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	DIT DBA		1-Jun-12
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
			DIT is currently performing daily backups of the PISTOL RMS application and database using CommVault. They perform a full backup once a week and incremental backups daily. The CommVault backups go to disk, then from disk to tape. See Attachment 1.
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
2	***The Police Department needs to invest in failover capability for the PISTOL RMS.***	Y	***RPD has the intention of purchasing new application and database servers and SQL software in the beginning of FY13 to include a second system to be installed at Police HQ for replication to provide failover for the PISTOL RMS. Target date is contingent on all purchase requisitions being approved expeditiously.***
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	RMS System Operations Administrator		30-Jun-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
3	***Remove or disable the default System Administrator account if it does not affect the system functionality.***	Y	***Disable System Administrator account***
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	RMS System Operations Administrator		20-Jun-12
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
			System Administrator account has been disabled.
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
4	***Restrict the users in “ALLRIGHTS” group to PISTOL RMS Administrator and backups.***	Y	***Remove TuttlePC from "ALLRIGHTS"group.***
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	RMS System Operations Administrator		20-Jun-12
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
			Removed user TUTTLEPC from "ALLRIGHTS" group leaving PISTOL RMS Administrator, RPD head of IT, vendor account, and 2 backups

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
5	***Ensure that MFR functions in the Police cars even if the connection between DEC and the City Hall is lost.***	Y	
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		6/1/2012
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
			MFR does currently function in the police cars with or without a network connection. If the MDTs do not have network capability, the officers can write reports in an OFFLINE mode then submit them via WIFI at the city's wireless hotspots or save them on a usb drive and upload them onto a precinct machine for supervisor review.

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
6	***Turn on password expiration and complexity settings for the PISTOL RMS application.***	Y	***Inform all PISTOL users that password complexity and expiration settings will be enabled as of 1/1/2013. Put changes into place in PISTOL System Configuration.***
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
7	***Upgrade the PISTOL SQL database to SQL2008.***	Y	***RPD has the intention of purchasing new application and database hardware and software to include SQL2008 in beginning of FY13. Install and implementation should be completed by target date.***
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		30-Jun-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
8	***Develop performance indicators for • Average time for resolution of major and minor application issues; • Number of incidents reopened; and • Percentage of incidents not resolved within the agreed upon timelines.***	Y	***RPD will develop a new comprehensive system administration manual for the PISTOL records management system and issue related general orders. RPD will include performance indicators and tracking for vendor response in the new RMS administration policy.***
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
9	***Establish a formal written security policy outlining the approval requirements for granting, modifying and removing access to PISTOL using least privilege principle (minimum level of access).***	Y	***RPD will develop a new comprehensive system administration manual for the PISTOL records management system and issue related general orders. RPD will develop and include a formal security policy for user access to PISTOL in the RMS administration policy and draft a General Order for approval and dissemination of this policy to all Personnel.***
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
10	***Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for PISTOL application users.***	Y	***RPD will develop a new comprehensive system administration manual for the records management system and issue related general orders. RPD will include the policies and procedures for access authentication controls in the RMS administration manual and draft a General Order for approval and dissemination of this policy to all Personnel. Policy and G.O. should be issued by target date.***
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
11	***Develop policies and procedures for managing changes, including minor application changes, major application changes and software releases. This should include procedures for testing and receiving proper authorization and are supported by a change request document.***	Y	***RPD will develop a new comprehensive system administration manual for the records management system and issue related general orders. RPD will include the policies and procedures for change control in the RMS administration manual. Policy should be issued by target date.***
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS

12	***Document the results of the periodic review of user access to PISTOL and actions taken to address the issues, if any.***	Y	***RPD will develop a new comprehensive system administration manual for the records management system and issue related general orders. RPD will include the policies and procedures for audit reviews in the RMS administration manual. Policy should be issued by target date.***
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
13	***Evaluate the cost- benefit of purchasing the E-Ticketing module. If the cost is beneficial, purchase and implement Pistol E-Ticketing module.***	Y	***RPD will complete a cost/benefit analysis to determine feasibility of implementing E-Ticketing.***
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	RMS System Operations Administrator		1-Jan-13
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
	RPD has received quote from our vendor for purchase - initial cost not including supplies and support is $645,000 plus $25,000 in annual maintenance fees.		