




20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

Date: June 17, 2010

To: Audit & Finance Committee

From: Jennifer Ruttman, City Auditor 

Subject: Review of the Municipal Court C-Cure Electronic Building Access System Management

cc: Matt Tafoya, Presiding City Magistrate
Paul Thomas, Court Administrator
Albert Lemke, Deputy Court Administrator
Trisha Sorensen, Asst. to the City Manager

The City Auditor's office has completed a review of the Municipal Court C-Cure Electronic Building Access System Management. Attached please find the report, the Court's response, and a memo explaining our position regarding the one issue on which consensus could not be reached. The report contains 7 recommendations, 4 of which have been implemented by the Court. Should you have any questions or comments, please do not hesitate to contact me at x3767.

SPECIAL REPORT

CITY AUDITOR

Report Date: June 17, 2010

Department: Mesa Municipal Court

Subject: Review of C-Cure Electronic Building Access System Management

PURPOSE

The City Auditor's office is responsible for ensuring that all reports received through the City of Mesa Fraud & Ethics Hotline are adequately investigated. During a 2009 Hotline investigation regarding overtime use at the Mesa Municipal Court, we discovered control weaknesses in the administration of the Court's building access security system (C-Cure). These weaknesses hindered our investigation and, more importantly, represent operational inefficiency and increased risks to data integrity and physical security.

OBJECTIVES

The objectives of this review were to identify the key risks associated with the administration and configuration of the Court's electronic building access security system and to make recommendations for reducing those risks.

SCOPE & METHODOLOGY

To accomplish our objectives, we:

- Interviewed employees of the Court, Municipal Security, PD-IT, ITD, the City Prosecutor and the City Attorney.
- Reviewed relevant City policies and procedures.
- Reviewed relevant documents produced by the AZ Supreme Court Administrative Office of the Courts (AOC), and relied on the City Attorney's interpretation of those documents.
- Consulted with IT security professionals with specific expertise in the areas of physical, logical and operational security systems administration.

BACKGROUND

The C-Cure system is used citywide to manage access control at various City buildings. This system is administered by a limited number of civilian employees in the Municipal Security and PDIT sections of the Police Department; however, the Court independently maintains and administers an entirely separate C-Cure system. The Court has maintained that any involvement by Police Department employees in the administration of their system represents a conflict of interest, or the appearance thereof, resulting in unacceptable risk to data integrity and public confidence.

Our findings and recommendations were discussed with the Court in February 2010, just as the new Court building was opening. At that time, we learned that as part of the transition to the

new facility, the Court had already made some operational changes in security administration which resolved some of our findings. The most significant of these changes was that the exterior perimeter C-Cure access points at the Court are now administered as part of the citywide system. However, all interior access points are still on a separate system maintained by the Court. The findings and recommendations presented in this report have been revised to be consistent with current operations as of February 2010. Issuance of the report was delayed until June, to allow management additional time to consider its options.

SUMMARY CONCLUSION

In our opinion, the Court's administration of a separate C-Cure system is inefficient and unjustified. We also found that no procedures were in place for monitoring, backups, business continuity disruptions or general system administration. In addition, we disagree with the Court's basis for its position with regard to system administration by Municipal Security and PDIT. It is our opinion that the Court can ensure the integrity of its systems while streamlining operations, maximizing efficiency and minimizing costs, by allowing the City to administer all C-Cure access points with a single system, with enhanced protocols for system monitoring and reporting. Our specific findings and recommendations are listed below.

FINDINGS & RECOMMENDATIONS

Finding #1

The Court's C-Cure system runs on a standard PC located in an office environment, without the benefits of increased stability and security offered by a server-based system and without the physical protection offered by a data center. In addition, there is no uninterruptable power supply (UPS) in use to protect the system in the event of a power failure; and the system is not backed up to a server or other off-site location. These conditions increase the risk to continuity of operations due to system failure; as well as the risk to data integrity due to security breaches. Furthermore, having this separate system duplicates several thousand dollars in costs associated with system administration, licensing and maintenance.

Recommendations:

- 1-1. The Court's C-Cure system should be run from the same secure server (located in a City Data Center) that houses the citywide system, thereby eliminating the Court's separate instance of the application.
- 1-2. All C-Cure data files should be backed up regularly and back-up files should be stored securely off-site.

Finding #2

Court-administered C-Cure access points are not monitored during non-business hours; therefore, a breach of one of these points may not be detected in a timely manner. Although the risks

associated with this finding were reduced when the exterior perimeter access points were placed on the citywide system in February, the interior access points should also be monitored.

Recommendation:

- 2-1. All C-Cure system access points should be monitored during non-business hours; so that security personnel can respond in a timely manner if any access point is breached.

Finding #3

At the time of our review, and as of February 2010, the Court's C-Cure system and its data were managed by and accessible to only one Court employee. This employee was responsible for authorizing access rights and executing that action in the system, duties which should be segregated as a standard internal control. This was also the only employee who could run reports from that system. There were no formal policies and procedures in place to govern these activities and access changes were not documented. In addition, there was no contingency plan in place to manage the system if this employee were to suddenly become unavailable. This lack of independent oversight increases the risk that data integrity could be compromised without detection and it limits the City's ability to conduct independent administrative investigations into the activities of its employees.

Recommendations:

- 3-1. C-Cure system administrator responsibilities should be shared by two or more individuals.
- 3-2. Changes to any individual's access should require the expressed written consent of an authorized employee who is not a C-Cure system administrator.
- 3-3. Documentation for all authorized changes should be placed in a single location and maintained in accordance with the City's document retention policies.
- 3-4. Court employees designated by the Presiding Magistrate, as well as Municipal Security C-Cure administrators, should have the ability to generate activity reports for all C-Cure access points at the Court. To ensure data integrity, these individuals should also have the ability to view system audit logs. This provides both internal and independent oversight, which are essential controls to ensure transparency and accountability.



250 East First Avenue
Mesa, Arizona 85210

mesaaz.gov

MEMORANDUM

June 16, 2010

TO: Jennifer Ruttman, City Auditor
FR: J. Matias Tafoya, Presiding Judge *JMT*
RE: C-Cure Special Report

Please find attached the Court response to recommendations as indicated in your report. We are appreciative and find it beneficial to have identified certain security concerns as a result of your report. However, the fundamental issue of Court retention of controlling access to Court areas may continue to be challenging. As per our discussion, we are satisfied that issues raised in your report have been substantially and successfully complied with in the range of 80 to 90 percent. Ultimately, final review and direction as to compliance rests with the Presiding Superior Court Judge and the Arizona Supreme Court Administrative Office of the Courts. Accordingly, we will be sharing your report with them in seeking further discussion on this subject.

AUDIT RESPONSE FORM
Mesa Municipal Court - Review of C-Cure System - May/2010

All of the recommendations made in our report are listed below. Following each recommendation, please provide the information requested. The space will expand, if necessary, to fit your text. Please e-mail the completed form to Jennifer.Ruttman@mesaaz.gov by June 7, 2010. Thank you.

FINDING #1

Recommendation #1-1. The Court's C-Cure system should be run from the same secure server (located in a City Data Center) that houses the citywide system, thereby eliminating the Court's separate instance of the application.		
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Disagree	The Court's current C-Cure system, along with the other recommendations already implemented, are sufficient for the needs of the Court.	
Recommendation #1-2. All C-Cure data files should be backed up regularly and back-up files should be stored securely off-site.		
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Agree	The Court will regularly back-up the C-Cure data files and store them off-site in a secure location.	

FINDING #2

Recommendation #2-1. All C-Cure system access points should be monitored during non-business hours; so that security personnel can respond in a timely manner if any access point is breached.		
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Agree	All exterior door access points are monitored during non-business hours by Municipal Security. Interior Court access points do not need to be monitored during non-business hours as an exterior access point would need to be breached before any interior access point can be breached.	

AUDIT RESPONSE FORM
Mesa Municipal Court - Review of C-Cure System - May/2010

FINDING #3


Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Agree	C-Cure system administrator responsibilities should be shared by two or more individuals. This recommendation has been implemented.	
Recommendation #3-2.	Changes to any individual's access should require the expressed <u>written</u> consent of an authorized employee who is not a C-Cure system administrator.	
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Agree	This recommendation has been implemented.	
Recommendation #3-3.	Documentation for all authorized changes should be placed in a single location and maintained in accordance with the City's document retention policies.	
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Agree	This recommendation has been implemented.	
Recommendation #3-4.	Court employees designated by the Presiding Magistrate, as well as Municipal Security C-Cure administrators, should have the ability to generate activity reports for all C-Cure access points at the Court. To ensure data integrity, these individuals should also have the ability to view system audit logs. This provides both internal and independent oversight, which are essential controls to ensure transparency and accountability.	
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Disagree	This recommendation has been implemented. The Court is governed by the Supreme Court's Records Retention Schedule (Administrative Code, Chapter 4 § 3.402), as acknowledged in the City's records management policy.	
Recommendation #3-4.	Court employees designated by the Presiding Magistrate, as well as Municipal Security C-Cure administrators, should have the ability to generate activity reports for all C-Cure access points at the Court. To ensure data integrity, these individuals should also have the ability to view system audit logs. This provides both internal and independent oversight, which are essential controls to ensure transparency and accountability.	
Agree Or Disagree	Brief Summary of Implementation Plan (NOTE: If recommendation will not be implemented, please explain your alternative plan to address the observation.)	Estimated Implementation Date (Month/Yr)
Disagree	The Court has implemented procedures and designated more than one system administrator for the C-Cure system. Since the Court's C-Cure system will be run from a separate computer, Municipal Security will not have a need to access or generate reports from the Court's C-Cure system.	



20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

Date: June 17, 2010

To: Audit & Finance Committee

From: Jennifer Ruttman, City Auditor 

Subject: Review of the Municipal Court C-Cure Electronic Building Access System Management – **Explanatory Memo re Court's Response**

The Court has elected not to implement our recommendation to consolidate their building access security system with the system used to manage access to other City buildings, citing the need for a separate security system for its interior doors. This position is based on the premise that a conflict of interest, in fact or appearance, would arise if Municipal Security and PDIT, under the supervision of the Police Department, were to maintain the Court's C-Cure system. We respectfully disagree; and we offer the following explanation of our position.

The vast majority of people who enter the Court building must first be screened and granted entry by a team of Municipal Security Officers who maintain a constant presence at the Court. If this does not create the appearance that the Police Department controls access to the Court, surely a group of system technicians who are never viewed by the public present no greater threat of an appearance of a conflict of interest.

Municipal Security and PDIT are civilian support units staffed by technical professionals, not by sworn police officers. These are civilian employees with no greater interest in Court access than any other employee, contractor or citizen. In addition, there are well established controls and organizational boundaries to preclude any undue influence by sworn personnel who would seek to gain unauthorized access to the Court. Even in the unlikely event that such a situation could arise, sophisticated monitoring tools and procedures would enable the Court to detect the anomaly.

Given the lack of consensus with regard to our recommendation to consolidate the two C-Cure systems, we have agreed to disagree and the Court has accepted responsibility for the associated risks, which include:

- Licensing and maintenance costs associated with a second system.
- Desktop setup not as secure and stable as a server-based configuration.
- No monitoring of interior access points during non-business hours.

However, as noted in the Court's response, many of the risks identified in our review have been successfully mitigated with new procedures and system changes. For example, the Court has agreed to:

- Perform regular backups of C-Cure data files.
- Utilize an uninterruptible power supply (UPS).
- Allow perimeter doors to be managed and monitored by Municipal Security.
- Ensure multiple individuals have access to the system.
- Implement procedures to document system changes and the related authorizations.

Our Mission: *The City Auditor's office provides audit, consulting, and investigative services to identify and minimize risks, maximize efficiencies, improve internal controls and strengthen Mesa's accountability to its citizens.*

Scheduled Audits for 2010/2011

Neighborhood Services – CDBG & HOME Programs	<ul style="list-style-type: none"> Verify that these programs are operating efficiently and in accordance with applicable regulations. Verify that adequate controls are in place and operating effectively to prevent or detect errors, fraud, waste and/or abuse.
Citywide – Grants Management Processes	<ul style="list-style-type: none"> Evaluate the efficiency and effectiveness of the City's grants management processes.
Court – Electronic Monitoring Program	<ul style="list-style-type: none"> Evaluate the cost effectiveness of the Electronic Monitoring (Ankle Bracelet) Program.
Citywide – Procurement Card Program	<ul style="list-style-type: none"> Evaluate procurement card use citywide for compliance with applicable policies and procedures. Verify that adequate controls are in place and operating effectively to prevent or detect errors, fraud, waste and/or abuse.
Citywide – Use of Temporary Labor and Personal Services Contracts	<ul style="list-style-type: none"> Evaluate the use of temporary agency workers and personal services contractors citywide for compliance with applicable policies and regulations. Verify that adequate controls are in place and operating effectively to ensure the costs associated with the use of temporary agency workers and personal services contractors are reasonable and appropriately managed.
Fleet Services – Procurement of Parts and Services	<ul style="list-style-type: none"> Evaluate the processes used by Fleet Services to procure parts and services for compliance with applicable policies and regulations. Verify that adequate controls are in place and operating effectively to prevent or detect fraud, waste, and/or abuse of resources.
Citywide – Use of State Contracts and Cooperative Agreements	<ul style="list-style-type: none"> Verify that adequate controls are in place and operating effectively to ensure that state contracts and cooperative agreements are used only when they provide the best value for the City.
Special requests	<ul style="list-style-type: none"> Special requests may require immediate attention and may supersede a scheduled audit.

On-Going Audits from 2009/2010 Audit Plan

Citywide – Stimulus Funds	Verify that the City has processes and controls in place to ensure that all stimulus funds are used appropriately and properly accounted for, and that all reporting requirements are met.
Financial Services – Bond Proceeds	Verify that proceeds from bonds with attached secondary property taxes were expended only for the intended voter-approved purposes.
Purchasing Division – Request For Proposal/Bid Process	Evaluate the request for proposal/bid process for adequate controls, compliance with applicable regulations, and for effectiveness in providing the best value for the City.

