AUDIT DEPARTMENT

Audit Report

Water Reclamation District Computer Operations Center Security and Infrastructure Follow Up Audit

October 2012

Angela M. Darragh, CPA, CISA, CFE
Audit Director

AUDIT COMMITTEE:
Commissioner Steve Sisolak
Commissioner Chris Giunchigliani
Commissioner Lawrence Weekly

Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

October 4, 2012

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

Pursuant to Audit Department policy, we performed follow-up procedures on the *Clark County Water Reclamation District Computer Operations Center Security and Infrastructure* audit. This follow-up letter should be read in conjunction with the original audit. The follow-up procedures we performed included interviews with responsible parties, a tour of communications closets, and an examination of related documentation. This follow-up engagement does not represent a complete reexamination of the original audit.

The auditor's role in follow-up engagements is to compile corrective actions taken from affected Department/Division management, assess whether these responses are adequate or not adequate to correct reported deficiencies, and relay those findings to management.

It is management's responsibility to decide if any appropriate action should be taken in response to reported audit findings. It is also management's responsibility to assume the risk of not correcting a reported condition because of cost or other consideration.

The results of our follow-up procedures showed that the District has taken corrective action on all findings that required follow up or chosen to accept the risk based on cost to correct the deficiencies.

The assistance and cooperation of the Clark County Water Reclamation District staff is recognized and appreciated.

Sincerely,

/s/ Angela M. Darragh

Angela M. Darragh, CPA
Audit Director

BOARD OF COUNTY COMMISSIONERS
SUSAN BRAGER, Chair • STEVE SISOLAK, Vice Chair
LARRY BROWN • TOM COLLINS • CHRIS GIUNCHIGLIANI • MARY BETH SCOW • LAWRENCE WEEKLY
DON BURNETTE, County Manager

TABLE OF CONTENTS

BACKGROUND 3

OBJECTIVES, SCOPE, AND METHODOLOGY 3

RESULTS OF FOLLOW-UP AUDIT 3

Implementation Rate 3

BACKGROUND

Clark County Audit Department performed an audit of the Water Reclamation District Computer Operations Center Security and Infrastructure dated October 1, 2010, for the period April 13, 2010, through July 8, 2010.

The results of the original audit identified several areas that needed corrective action. The results in brief indicated the following concerns:

- Fire Suppression Systems
- Access and Processing Controls
- Data Back-up and Recovery Procedures
- Environment Controls
- Policies and Procedures

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this follow-up audit is to determine whether adequate corrective action was taken on the findings noted in the original audit.

Our procedures consisted of reviewing the original audit report and supporting work papers, interviews with responsible management and staff, observations of communications closets, and examination of policies and procedures and other related documentation. The last day of fieldwork was August 17, 2012.

We conducted this performance audit 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.

RESULTS OF FOLLOW-UP AUDIT

The District has taken adequate corrective action on all findings that required follow-up.

Implementation Rate

Status of Findings	Number of Findings	% of Total
Implemented	9	75%
Not Implemented	0	0%
Other	3	25%
Total	12	100%

Clark County Water Reclamation District
Computer Operations Center Follow-Up Audit
Findings, Recommendations, and Corrective Actions Status
As of August 17, 2012

AUDIT DEPARTMENT
Angela M. Darragh, CPA, CFE, CISA
Audit Director

Original Report Issuance Date: October 1, 2010

Summary Audit Findings & Recommendations			Summary Management Response		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Action Status	Implemented	Not Implemented	Other
1	**Fire Suppression System**						
	A FM-200 fire suppression system was installed in the CCWRD administration building to protect the computer room. During the walk-through, it was noted that the system was disconnected and the inspection tags were out-of-date.	It is recommended that management should have the FM-200 system inspected and reconnected.	Y	The FM-200 fire suppression system has been inspected and reconnected.	✓		
2	**Fire Suppression System-Other IT Areas**						
	The communications closets had water-based sprinkler systems and the Desert Breeze facility, that is used for off-site data backup and recovery storage, had no fire suppression system in the room used to store the tapes.	It is recommended that management should install small space FM-200 systems in each of these areas.	Y	According to management, the cost to install a small space FM-200 system can be as high as $100,000. The cost of the equipment maintained in the closets is between $20,000 and $50,000. The cost of the fire system exceeds the benefit; therefore, management has elected to not install a FM-200 system in these areas. Management provided a cost analysis comparing the equipment cost to the cost of a FM200 system. The amounts quoted by management are reasonable and we agree with their conclusion. Additionally, the data backup tapes are stored in a fire proof safe at the Desert Breeze facility.			✓
3	**Access Controls-Computer Room**						
	There are 138 individuals who have a proximity card-key access to the computer server room.	It is recommended that management should limit access to the computer room to Information Technology server administration personnel, security personnel and their managers.	Y	Access to the computer and communications equipment has been restricted to necessary personnel only.	✓		

Summary Audit Findings & Recommendations			Summary Management Response		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Action Status	Implemented	Not Implemented	Other
4	**Data Back-up and Recovery**						
	The cabinet to house the current month's back-up tapes is located inside the computer room. Any event impacting the computer room would also impact the current back-up tapes. There is no fire protection in the room used to store the back-up tapes at the Desert Breeze facility.	It is recommended that management should move the lateral cabinet used to store in-house data back-up tapes from the computer room to the communications closet. At the Desert Breeze facility, a fire rated cabinet should be used to store back-up tapes, a dry FM-200 small space fire suppression system should be installed, and a printed copy of the current tape inventory should be stored with the back-up tapes.	Y	The lateral cabinet has been moved, a fire rated safe is located at the Desert Breeze facility to store back-up tapes, and a tape inventory is maintained. The District has elected to not install a dry FM-200 fire suppression system, but the back-up tapes are stored in the fire rated safe.			✓
5	**Environment Control IDF 188 Communications**						
	The first floor communications closet contains three components, a network hub, a telephone system patch panel, and security system control components. The fire suppression system in the closet is water based and the space is used for office supply and general storage.	It is recommended that the closet is not used for storage, a small space FM-200 system should be installed, and access to the closet should be limited to Information Technology technical support personnel and security personnel.	Y	The room has been cleaned and is not used for storage. Access has been restricted to appropriate personnel. Management is in the preliminary stage of placing a FM-200 system in the communications closet.			✓
6	**Environment Control IDF 217 Communications**						
	The attic access port in the ceiling was not covered, the closet is used to store materials for classroom demonstrations, and the closet is equipped with a water base fire suppression system.	It is recommended that the closet is not used for storage, a small space FM-200 system should be installed, the ceiling access port should be covered, firmly secured, and access to the closet should be limited to Information Technology technical support personnel and security personnel.	Y	The closet has been cleaned of all storage items and the ceiling port has been covered and secured. Management has elected to not install a small space dry FM-200 system in this space.	✓		

Summary Audit Findings & Recommendations			Summary Management Response		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Action Status	Implemented	Not Implemented	Other
7	**Telephone Room**						
	The telephone room was being used for what appeared to be temporary storage for various materials ranging from boxes full of reclaimed telephones to miscellaneous combustible materials.	It is recommended that management should ensure the telephone room is cleared of all non-essential and non-communications related materials. They should ensure that all materials are appropriately stored in enclosed cabinets, lockers, and/or desks. Once the room has been cleared, it should be cleaned.	Y	The room has been cleared of all non-essential and non-communications related materials. The room has been cleaned.	✓		
8	**Server Room**						
	The server room is exposed to an environmental hazard due to its neighboring work space-room 173. This room was designed to be a receiving area for equipment used in the server room. As such, there are double doors that open outside the building and a double door size folding door that separates room 173 from the server room. Neither sets of doors provides an effective seal to prevent dust intrusion.	It is recommended that management have appropriate devices installed on the double doors in room 179 to prevent air leaks that allow dust to enter the room.	Y	The double door in the storage room 179 has been replaced with a steel roll up door that seals properly and prevents air leaks from the outside.	✓		
9	**Room 173 Storage**						
	The storage room adjacent to the server room was filled with new and used equipment to the point where moving about the room was difficult. The room was dusty.	It is recommended that management find more appropriate storage, in a clean area, that can be used to store components waiting to installed or released.	Y	The storage room has been cleaned and organized.	✓		
10	**Server Room Carpet**						
	The server room has carpet which introduces a risk of static electricity.	It is recommended that the carpet squares covering the computer room floor is removed and if necessary replaced with raised floor tiles.	Y	The carpet squares covering the computer room floor have been removed.	✓		

Summary Audit Findings & Recommendations			Summary Management Response		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Action Status	Implemented	Not Implemented	Other
11	**Room 173 Pass-Through**						
	The pass-through door between the server room and the storage room cannot maintain containment should the FM-200 fire suppression system discharge occur.	It is recommended that management replace the current closure between the server room and the storage room with doors that are capable of maintaining a seal that will prevent the passage of air between the two rooms. The doors should be firmly seated to ensure that they cannot be blown open during a FM-200 discharge.	Y	The door has been replaced and now properly seals and prevents the passage of air between the two rooms.	✓		
12	**Policies and Procedures**						
	The Water Reclamation District Information Technology Department has published 39 policy statements directly related to their operations. Our review noted five minor exposures in these policies that could weaken the overall control environment.	Management should consider making the following adjustments to their IT Policies: 1. Policy 22 - Media Disposal. - CCWRD should include paper as a media; Paper should be shredded. 2. Policy 24 - Mobile Computing Devices - CCWRD should add an encryption requirement to this policy. 3. Policy 27 - Personal Digital Assistant (PDA) Service and Support Policy – CCWRD should add an encryption requirement to this policy. 4. Policy 28 - Peer to Peer File Sharing (P2P) - CCWRD should add Instant Messaging guidance to this policy. 5. Policy 35 - Systems Network Monitoring Policy - CCWRD should include a required PCI level review periodically across all Server platforms in this policy.	Y	Management has updated all five policies as recommended.	✓		