SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

906

FROM: County Auditor-Controller

SUBMITTAL DATE:
March 8, 2006

SUBJECT: Internal Auditor's Letter #2006-302 – Department of Veterans Services Follow-up Review

RECOMMENDED MOTION: Receive and file the Internal Auditor's Letter.

BACKGROUND: The Auditor-Controller completed a review of the Veterans Services Department. Our primary objective was to determine if management implemented corrective action in response to the Finding 1 and Recommendation 1 from Internal Auditor's Report #2005-007, dated June 7, 2005.

Based upon the results of our review, the department has complied with Recommendation 1 and has implemented the usage of a secured locked media chest to better safeguard and limit access to customer's confidential information.

Departmental Concurrence

for Robert E. Byrd
County Auditor-Controller

FINANCIAL DATA				
	Current F.Y. Total Cost:	$ 0	In Current Year Budget:	N/A
	Current F.Y. Net County Cost:	$ 0	Budget Adjustment:	N/A
	Annual Net County Cost:	$ 0	For Fiscal Year:	N/A

SOURCE OF FUNDS: N/A

Positions To Be Deleted Per A-30 ☐

Requires 4/5 Vote ☐

C.E.O. RECOMMENDATION: RECEIVE & FILE

County Executive Office Signature

Dep't Recomm.: ☐ Consent ☐ Policy
Per Exec. Ofc.: ☒ Consent ☐ Policy

Prev. Agn. Ref.: | **District:** | **Agenda Number:** 2.4

OFFICE OF THE
COUNTY AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802

COUNTY OF RIVERSIDE
AUDITOR-CONTROLLER

Robert E. Byrd, CGFM
AUDITOR-CONTROLLER

Ivan M. Chand, CGFM
ASSISTANT AUDITOR-CONTROLLER

March 8, 2006

Mr. William H. Densmore, Director
Department of Veterans Services
1153A Spruce Street
Riverside, CA 92507

Subject: Internal Auditor's Report #2006-302 Veterans' Services Follow-Up Review

Dear Mr. Densmore:

We have completed a follow-up review of the Department of Veterans' Services. Our primary objective was to determine if management implemented corrective action in response to the Finding 1 and Recommendation 1 from Internal Auditor's Report #2005-007, dated June 2, 2005.

Our review consisted of communications with you and an evaluation of pertinent information relative to the findings reported in Internal Auditor's Report #2005-007.

During our initial audit we determined confidential information was not properly safeguarded. As a means of off-site storage, a designated employee maintained possession of the Veterans Information Database backup micro-tape overnight; therefore, increasing accessibility to confidential information, such as, veteran's social security numbers, dates of birth and service numbers. As a result, we recommended the Department consider storing database backup tapes at a secure off-site location.

According to the Privacy Act of 1974 Section 552a.(e)(10), an agency shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. Without properly safeguarding and limiting access to confidential information, the potential for loss, theft or misuse of confidential information exists. According to the Federal Trade Commission (FTC), 516,740 fraud and identity theft complaints were reported nationwide during the 2003 calendar year, resulting in consumers' reported losses of more than $400 million. In a comparison of major metropolitan areas nationwide, the FTC also reported the Riverside-San Bernardino area as having the third highest incidence of identity theft, exceeded only by Phoenix and Los Angeles.

In our communications with you as part of our preparation for this follow-up review, you indicated that options are being explored to store the backup tapes; however a corrective action has not yet occurred.

In light of the information at risk and the potential negative impact to your customers, we believe our recommendation should have already been implemented to better safeguard and limit access to confidential information. We further recommend that you consult with the County's Information Security Officer in the process of developing a backup system that will be sufficient to protect the information in question.

Management's Reply

Recommendation #1 of the abovementioned Internal Auditor's Report #2005-007 instructed my department to "Properly safeguard and limit access to confidential information," and recommended we "Consider storing database backup tapes at a secure off-site location." My formal 04-18-05 response to that recommendation advised that I would be reviewing several options but would for the time being budget "for the purchase of a suitable safe to be kept in our Riverside office."

Prior to the 2006 internal audit, the department's practice was to nightly backup our database and have a trusted employee take the backup tapes offsite (home), to be returned the next working day. As a result of your Report #2005-007 we started placing the backup tapes in an unlocked container kept in the Workforce Development Center's locked computer room where our server is located. I felt this was a reasonable interim solution because not only are the WDC's outside doors locked after hours but access to the computer room is extremely limited through a combination-locked door.

After consulting with Wayne Beckham of the County's Information Security Office, we are adding the following safeguard: we are presently purchasing an Office Max Media Chest ("fire protection for computer/magnetic media products") for $269.12. Hereinafter, our nightly backup tapes will be placed in the locked media chest and stored in the WDC's computer room. I believe this solution is both affordable and complies with the letter and intent of Recommendation #1. While the solution begs the question of tape loss with building destruction, it does satisfy the primary requirement of protecting client data.

Auditor's Comment

We are satisfied with the corrective action taken.

ROBERT E. BYRD, CGFM
Auditor-Controller

Rachelle Roman

for By: Michael G. Alexander, MBA, CIA
Chief Internal Auditor

Cc: Board of Supervisors
County Counsel
Lisa Brandl, Executive Office

COUNTY OF RIVERSIDE
DEPARTMENT OF VETERANS' SERVICES
WILLIAM H. DENSMORE, DIRECTOR

MAIN OFFICE:
1153A SPRUCE STREET
RIVERSIDE, CALIFORNIA 92507-2428
TELEPHONE: (951) 955-6050
FAX: (951) 955-6061
TTY: (951) 955-3098
TOLL FREE: 1-800-481-2101

BRANCH OFFICE:
880 N. STATE STREET, ROOM B-4
HEMET, CA 92543
TELEPHONE: (951) 766-2566
FAX: (951) 766-2567
TTY: (951) 955-3098
TOLL FREE: 1-800-481-2101

BRANCH OFFICE:
82-675 HIGHWAY 111, ROOM 120
INDIO, CALIFORNIA 92201
TELEPHONE: (760) 863-8268
FAX: (760) 863-8478
TTY: (951) 955-3098
TOLL FREE: 1-800-481-2101

MEMORANDUM

TO: Robert E. Byrd, CGFM
Riverside County Auditor-Controller

FROM: William H. Densmore, Director

DATE: March 3, 2006

SUBJ: **Internal Auditor's Report #2006-302 Veterans' Services Follow-up Review**

This letter is in response to:

1. Internal Auditor's Report #2005-007
2. Your Form 11 dated 06-02-05, and
3. Your draft Report #2006-302 date 02-14-06.

Recommendation #1 of the abovementioned Internal Auditor's Report #2005-007 instructed my department to "Properly safeguard and limit access to confidential information", and recommended we "Consider storing database backup tapes at a secure off-site location". My formal 04-18-05 response to that recommendation advised that I would be reviewing several options but would for the time being budget "for the purchase of a suitable safe to be kept in our Riverside office".

Prior to the 2005 internal audit, the department's practice was to nightly backup our database and have a trusted employee take the backup tapes offsite (home), to be returned the next working day. As a result of your Report #2005-007 we started placing the backup tapes in an unlocked container kept in the Workforce Development Center's locked computer room where our server is located. I felt this was a reasonable interim solution because not only are the WDC's outside doors locked after hours but access to the computer room is extremely limited through a combination-locked door.

After consulting with Wayne Beckham of the county's Information Security Office, we are adding the following safeguard: we are presently purchasing an Office Max Media Chest ("fire protection for computer/magnetic media products") for $269.12. Hereinafter, our nightly backup tapes will be placed in the locked media chest and stored in the WDC's computer room. I believe this solution is both affordable and complies with the letter and intent of

Recommendation #1. While the solution begs the question of tape loss with building destruction, it does satisfy the primary requirement of protecting client data.

Please contact me if you have any question.

WHD:eyg

Cc: Michael Alexander, Chief Internal Auditor
Tina Grande, Executive Office
Wayne Beckham, Information Security Office