

OFFICE OF AUDITS & ADVISORY SERVICES



SAFEGUARDS FOR CLIENT CONFIDENTIALITY – PUBLIC DEFENDER

FINAL AUDIT REPORT

Chief of Audits (Acting): [Thomas G. Philipp, CIA, CCSA](#)
Supervising Senior Auditor: [Yuki Matsuura, CPA, CCSA](#)
Auditor I: [Christopher Arias](#)

Intentionally Left Blank



County of San Diego

DONALD F. STEUER
CHIEF FINANCIAL OFFICER
(619) 531-5413
FAX (619) 531-5219

AUDITOR AND CONTROLLER
1600 PACIFIC HIGHWAY STE 166, SAN DIEGO, CALIFORNIA 92101-2478

TRACY M. SANDOVAL
ASST. CHIEF FINANCIAL OFFICER/
AUDITOR & CONTROLLER
(619) 531-5413
FAX (619) 531-5219

December 28, 2011

TO: Henry C. Coker, Public Defender
Office of the Public Defender

FROM: Thomas G. Philipp
Chief of Audits (Acting)

FINAL REPORT: SAFEGUARDS FOR CLIENT CONFIDENTIALITY – PUBLIC DEFENDER

Enclosed is our report on the audit of the Safeguards for Client Confidentiality – Public Defender. We have reviewed your responses to our recommendations and have attached them to the audit report. The actions taken are responsive to the recommendations in the report.

Thank you for the courtesousness and cooperation extended to the Office of Audits & Advisory Services during the course of the audit.

If you have any questions, please contact me at (858) 495-5665.

THOMAS G. PHILIPP
Chief of Audits (Acting)

AUD:YM:cta

Enclosure

c: Ronald J. Lane, Deputy Chief Administrative Officer, Public Safety Group
Donald F. Steuer, Chief Financial Officer
Tracy M. Sandoval, Assistant Chief Financial Officer/Auditor and Controller
Dorothy Y. Thrush, Group Finance Director, Public Safety Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of the Safeguards for Client Confidentiality – Public Defender. The objective of the audit was to determine whether the Office of the Public Defender (PD) has sufficient safeguards to ensure confidential, conflict-free representation.

Background

The PD provides legal assistance to individuals charged with a crime in State court who are financially unable to retain private counsel. When more than one person is charged with the commission of the same crime, it would be a conflict of interest for the PD to represent all defendants charged in the case. Defendants are entitled to conflict-free representation, which has been consistently interpreted in the Sixth Amendment Right to Counsel. Consequences of providing legal counsel despite a known conflict of interest include, but are not limited to, case reversal and state bar discipline up to and including disbarment.

To ensure conflict-free representation, four separate law offices exist within the PD: the Primary PD (PPD), Alternate PD (APD), Multiple Conflicts Office (MCO), and the Office of Assigned Counsel (OAC). These offices must operate separately and independently to maintain the “ethical walls” described in several court cases.

Audit Scope & Limitations

The scope of the audit included the following areas:

- Physical access to PD offices, with an emphasis on PD Headquarters at 450 “B” Street, San Diego, CA 92101;
- Logical access to departmental Home Folders (H:\Drive) and Group Folders (S:\Drive);
- Logical access to the Judicial Court Activity Tracking System (JCATS), PD’s case management system administered by Canyon Solutions, Inc.; and
- Retrieval of off-site PD case information maintained at Iron Mountain (IM) through the Documentum Records Manager (DRM) and IM Connect systems.

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors, as required by California Government Code, Section 1236.

Methodology

OAAS performed the audit using the following methods:

- Interviewed PD Administration, PPD, APD, MCO, and OAC management and staff to obtain an understanding of PD’s ethical

wall structure;

- Reviewed and compared the ethical wall criteria in PD's Policy and Procedure Manual to those described in several court cases;
- Assessed risks and controls independently and in coordination with PD management; and
- Performed detailed analysis on selected areas to determine whether the PD maintains sufficient safeguards to ensure:
 - Physical separation between the PPD, APD, MCO, and OAC to prevent unauthorized access by reviewing physical access information provided by the County Security Office;
 - Security over departmental H:\Drive and S:\Drive by interviewing Hewlett Packard and County Technology Office staff and reviewing supporting documentation for PD's control activities;
 - Security over JCATS to prevent unauthorized access and case modifications by reviewing system access information provided by the global JCATS Administrator at Canyon Solutions, Inc.; and
 - Security over off-site PD case information maintained at IM by interviewing staff of the Department of Purchasing & Contracting Records Services Division (P&C Records Services) and reviewing DRM/IM Connect access information.

AUDIT RESULTS

Summary

Within the scope of the audit, OAAS concluded that PD's ethical wall practices provide reasonable assurance that the PD has sufficient safeguards to ensure confidential, conflict-free representation. However, OAAS noted the following opportunity for improvement:

Finding:

The Ability to Retrieve Off-Site PD Case Information Should Be Limited to Properly Authorized PD Employees

Of the 48 DRM/IM Connect users with the ability to retrieve off-site PD case information, 10 (21%) users had an inappropriate level of access. Of these 10 users:

- Four users are current PD employees who were able to retrieve off-site PD case information belonging to other offices within the department. Based on a review of the IM Retrieval History Reports from June through October 2011, OAAS confirmed that these employees only retrieved off-site information belonging to their respective offices.

- Six users were not employed by the PD as of the review date, but are still employed by the County. Based on a review of the reports noted above, OAAS confirmed that these six users did not retrieve any off-site PD case information. Additionally, based on a review of JCATS user information provided by Canyon Solutions, it was confirmed that these six users did not have access to JCATS.

According to P&C Records Services' policies, departments are responsible for notifying them when an employee's DRM/IM Connect access needs to be modified and/or terminated.

PD management indicated that the DRM/IM Connect access for the four users above was established in error due to unclear communication between PD and P&C Records Services after the 2009 merger of the PD and the APD into one department. For the remaining six users above, the PD did not notify P&C Records Services to terminate their DRM/IM Connect access after they transferred to other County departments. There was no review or monitoring of authorized DRM/IM Connect users to ensure that access was limited to properly authorized PD employees.

PD management, upon reviewing the access rights of all 10 users noted above, subsequently requested that P&C Records Services modify and/or terminate these users' access. However, their current procedures may result in employees inappropriately retaining the ability to retrieve off-site PD case information after transferring or leaving the department.

Recommendation:

To strengthen the controls over the ability to retrieve off-site PD case information, PD management should:

1. Enhance current procedures to ensure that the P&C Records Services is notified of employee transfers and/or terminations as they occur so that their DRM/IM Connect access can be modified and/or terminated; and
2. Periodically monitor the list of authorized PD DRM/IM Connect users and verify that only properly authorized PD employees have the ability to retrieve off-site PD case information.

Office of Audits & Advisory Services

Compliance

Reliability

Effectiveness

Accountability

Transparency

Efficiency

VALUE

**DEPARTMENT'S RESPONSE
(OFFICE OF THE PUBLIC DEFENDER)**

PRIMARY PUBLIC DEFENDER
450 B Street, Suite 900
San Diego, CA 92101
619-338-4700
619-338-4811 FAX



ALTERNATE PUBLIC DEFENDER
450 B Street, Suite 1200
San Diego, CA 92101
619-446-2900
Fax: 619-446-2955

OFFICE OF ASSIGNED COUNSEL
450 B Street, Suite 840
San Diego, CA 92101
619-338-4800
Fax: 619-338-4743

County of San Diego
DEPARTMENT OF THE PUBLIC DEFENDER

MULTIPLE CONFLICTS OFFICE
450 B Street, Suite 1210
San Diego, CA 92101
619-446-2909
Fax: 619-446-2941

HENRY C. COKER
PUBLIC DEFENDER

December 20, 2011

RECEIVED

DEC 23 2011

**OFFICE OF AUDITS &
ADVISORY SERVICES**

TO: James L. Pelletier
Chief of Audits

FROM: Henry C. Coker, Public Defender, Department of the Public Defender

**DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: SAFEGUARDS FOR
CLIENT CONFIDENTIALITY-PUBLIC DEFENDER**

**Finding I: The Ability to Retrieve Off-Site PD Case Information Should Be Limited
to Properly Authorized PD Employees**

OAAS Recommendation:

To strengthen the controls over the ability to retrieve off-site PD case information, PD management should:

1. Enhance current procedures to ensure that the P&C Records Services is notified of employee transfers and/or terminations as they occur so that their DRM/IM Connect access can be modified and/or terminated; and
2. Periodically monitor the list of authorized PD DRM/IM Connect users and verify that only properly authorized PD employees have the ability to retrieve off-site PD case information.

Action Plan: The Department appreciates the effort put into the audit and concurs with the audit recommendations in their entirety.

As to recommendation number one, we are of the view that the Senior Department HR Manager should be responsible for notifying the Department IT Manager of all interoffice transfers and all terminations, and that the IT Manager should in turn notify P & C Records Services as to which access rights require change or termination.

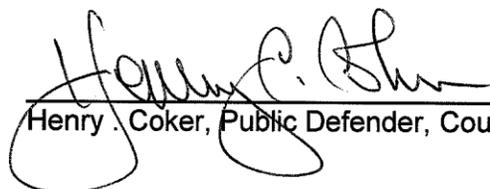
James L. Pelletier, Chief of Audits
Page 2
December 20, 2011

As to recommendation number two, we believe that the Department IT Manager should have the responsibility for monitoring the list of PD DRM/IM connect users every 90 days and verifying that only properly authorized users have the ability to retrieve off-site Public Defender case information.

Currently the Department IT Manager position is unfilled, and until the position is filled, The Director of Administrative Services and Finance, Steve Lujan, has been designated to temporarily stand in and perform the herein described duties of the Department IT Manager.

Contact Information for Implementation: Steve Lujan, Director of Administrative Services and Finance. (619-338-4714)

If you have any questions, please do not hesitate to contact me at:
619-338-4797



Henry Coker, Public Defender, County of San Diego

Confidentiality Notice: This E-mail transmission (and/or the documents accompanying it) is for the sole use of the intended recipient(s) and may contain information protected by the attorney-client privilege, the attorney work product doctrine or other applicable privileges or confidentiality laws or regulations. If you are not an intended recipient, you may not review, use, copy, disclose or distribute this message or any other information contained in this message to anyone. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of this message and any attachments