



Internal Audit
Department

301 W Jefferson
Suite 660
Phoenix, AZ 85003

[maricopa.gov/
internalaudit](http://maricopa.gov/internalaudit)
602.506.1585

Ross L. Tate
County Auditor

Adult Probation Department

June 2013

*Internal Audit Report Authorized by the
Maricopa County Board of Supervisors*

Report Highlights	Page
The Adult Probation Department (APD) will continue to ensure that Intensive Probation Supervision (IPS) caseload ratios comply with statute.	1
IPS risk assessments will be administered within guidelines.	2
IPS supervisory reviews will be performed in accordance with policy.	2
IPS case plans will be completed within required timeframes.	3
APD IT controls are consistent with recommended standards in many key areas.	8
APD is working with Court Technology Services to ensure law enforcement network security.	8

Audit Objectives

To determine that:

- Intensive probationers are properly monitored in accordance with select Arizona Code of Judicial Administration requirements and APD policies and procedures.
- IT general controls and critical application controls are effective.

Scope

We randomly selected 72 of 697 (10%) IPS probationers as of 12/30/11 for review. Our primary audit period was fiscal year 2012, although the items sampled and the audit period varied based upon the audit test being performed.

In order to achieve our objectives, we reviewed relevant Arizona Revised Statutes (A.R.S.), Arizona Code of Judicial Administration (ACJA) guidelines, and Adult Probation Department (APD) internal policies and procedures pertaining to intensive probationers. We also examined relevant records and IPS case files, reviewed relevant standards on intensive probation, and interviewed key personnel. Compliance with caseload limits was determined as of 12/31/11 and 6/30/12.

The IT objectives were focused on evaluating the effectiveness of IT general and application controls supporting APD Online, which is the application APD uses to aggregate and report data from the Adult Probation Enterprise Tracking System (APETS). Our primary audit period was fiscal year 2013, although some documentation under review covered prior periods. We assessed the APD end-user computing controls that supported APETS as of 9/30/12. In order to achieve our objectives, we reviewed critical APD Online controls to determine that they ensured data confidentiality, integrity, and availability.

Standards

This audit was approved by the Board of Supervisors and conforms to International Standards for the Professional Practice of Internal Auditing. The specific areas reviewed were selected through a formal, risk assessment process.

Audit Results

Issue #1: Intensive Probation Caseload Ratios

Observation: For the two periods reviewed, 21 of 108 (19%) Intensive Probation Supervision (IPS) officers had caseloads that exceeded 15 probationers, the maximum allowed by Administrative Directive No. 2012-16. Nine officers had caseloads ranging from 18 to 23 probationers.

Although the Adult Probation Department (APD) was exempted from probation ratios prescribed by law (A.R.S. § 13-916) with the passage of A.R.S. § 12-269 in 2006, APD signed an Adult Intensive Probation Team/Contact Standards Waiver Request, which stipulated that IPS officers would supervise no more than 15 cases each. The document was signed by APD's Chief Probation Officer and the Presiding Judge of the Superior Court in May 2012, and was approved by the Administrative Office of the Courts (AOC) with the issuance of Administrative Directive No. 2012-16 in July 2012. APD reports that the waiver is prepared by and signed at the request of the AOC annually.

APD asserts that they are fully compliant with caseload limit requirements because it is A.R.S. § 12-269, not Administrative Directive No. 2012-16, that controls probationer ratios. Specifically, A.R.S. § 12-269(B) requires only that APD "maintain appropriate ratios of officers to probationers consistent with evidence based practices in differentiated case management." While APD was in compliance with this statute on the dates reviewed, caseload ratios exceeded the limit specified in the above-referenced waiver and Administrative Directive No. 2012-16.

Conclusion #1A: IPS caseload ratios were in compliance with statute during the two periods reviewed, but exceeded the limit stipulated in Administrative Directive No. 2012-16.

Recommendation	APD Action Plan
1A-1 Review the issue with the AOC and determine the appropriate resolution.	Concur – in process. Pursuant to A.R.S. § 12-269(B), APD has the legal authority to "maintain appropriate ratios of officers to probationers consistent with evidence based practices in differentiated case management." The statute requires a County to maintain probation standards, and exempts the County from probation ratios as prescribed by law. APD will discuss this finding with the AOC. Target Date: 10/1/2013

Issue #2: Risk Assessments

Observation: IPS risk assessments were not always administered by APD within required timeframes. Eight of 69 (12%) sampled probationers did not have an initial risk assessment completed within 30 days of sentence, reinstatement, or release from jail, as required. Additionally, 39 of 150 (26%) risk assessments analyzed were administered late, and 31 of 55 (56%) sampled probationers had at least one past due risk assessment.

Conclusion #2A: IPS risk assessments were not always administered within required timeframes.	
Recommendation	APD Action Plan
2A-1 Establish an effective tracking system, including appropriate oversight, to help ensure that risk assessments are administered within required timeframes.	Concur – in process. APD Online will be consistently utilized by officers to monitor the due dates of risk assessments indicated by red notification dots. Target Date: 7/1/2013

Issue #3: Supervisory Reviews

Observation: IPS supervisory reviews were not performed in accordance with APD policy during the period reviewed. Supervisors did not observe the minimum number of Field Reassessment Offender Screening Tool (FROST) interviews for 26 of 29 (90%) probation officers reviewed, which included 17 officers with no FROST interview observations. In addition, the minimum number of cases was not reviewed for 4 of 27 (15%) officers, while the number of cases reviewed was not documented for an additional two officers (7%). Further, required documentation was not on file for 4 of 29 (14%) FROSTs observed.

Conclusion #3A: IPS supervisory reviews were not performed in accordance with APD policy.	
Recommendation	APD Action Plan
3A-1 Establish an effective tracking system, including appropriate oversight, to help ensure that supervisory reviews are performed in accordance with APD policy.	Concur – will implement with modifications. Policy 31.005 will be amended to require 3 annual observations, one of which will be a FROST, to comprehensively evaluate an officer. Supervisors will submit a monthly report form to their Division Director which will include the name of each officer and the number and type of observations.

Recommendation	APD Action Plan (Continued)
	<p>The monthly report form will record the number of case audits completed during the month.</p> <p>Target Date: 9/1/2013</p>

Issue #4: Case Plans

Observation: All IPS case plans reviewed included probationer risk/needs, as determined by the risk assessment, and contained measurable objectives. However, 22 of 69 (32%) were not completed within 30 days (average of 45 days *late*), as required, and 2 were not completed at all. Additionally, 25 of 69 (36%) did not contain all required signatures.

<p>Conclusion #4A: All IPS case plans reviewed incorporated probationer risk/needs and contained measurable objectives, as required.</p>	
Recommendation	APD Action Plan
None	N/A
<p>Conclusion #4B: Nearly a third of IPS case plans reviewed were not completed timely, two were not completed at all, and a third did not contain all required signatures.</p>	
Recommendation	APD Action Plan
<p>4B-1 Establish an effective tracking system, including appropriate oversight, to help ensure that case plans are completed within required timeframes and contain all required signatures.</p>	<p>Concur – in process.</p> <p>APD Online will be consistently utilized by officers to track the due dates of case plans indicated by red notification dots.</p> <p>The requirement for case plan signatures will be added to the case audit form for tracking during the case audit process.</p> <p>Target Date: 7/1/2013</p>

Issue #5: Employment and Student Status Verification

Observation: While Employer Notification letters were sent out within the required timeframe for 26 of 40 (65%) IPS probationers reviewed, 9 were sent late, and 5 were not sent at all. Additionally, probation officers did not perform weekly follow up with employers to obtain the signed letters for 7 of 8 (88%) cases reviewed, and 46 of 380 (12%) recorded employer contacts were not made at the required interval. Additionally, student status was not properly verified for 8 of 10 (80%) probationers reviewed.

Conclusion #5A: IPS compliance with employer notification and student verification requirements needs to be improved.	
Recommendation	APD Action Plan
5A-1 Establish an effective tracking system, including appropriate oversight, to help ensure compliance with employment and student verification requirements.	<p>Concur – in process.</p> <p>Compliance with employment letter timeframes, follow-up and employer contacts will be monitored during the case audit process. Case audits will be reported on the supervisor monthly report form which is submitted to the Division Director.</p> <p>Policy 31.003 will be amended to include specific school verification criteria. A final grade report will be required at the end of a semester.</p> <p>Target Date: 7/1/2013</p>

Issue #6: Referrals to Services and Treatment

Observation: APD was in compliance with many IPS referral requirements reviewed, but improvement could be made. For instance, 45 of 47 (96%) written referrals to service providers reviewed were provided within the required timeframe. Additionally, enrollment in treatment programs was verified for 49 of 52 (94%) sampled probationers who received services, and completion of treatment was verified for 14 of 15 (93%) probationers who completed treatment during the review period. However, while case notes indicated referrals were provided verbally in all 53 cases, written referrals were not provided to 6 of 53 (11%) IPS probationers, as required. Of the written referrals provided, 8 of 47 (17%) did not contain the required program contact information and/or the date by which screening/entry should be accomplished. Finally, signed Consent for Release of Information forms were not on file for 8 of 53 (15%) cases.

Conclusion #6A: While most IPS probationers were referred to and received services, probation officers did not always comply with written referral requirements.	
Recommendation	APD Action Plan
6A-1 Provide officer training to help ensure compliance with all referral requirements.	<p>Concur – in process.</p> <p>APD provided 83% comprehensive written referrals to service providers. The next IPS Forum will include training on the importance of providing thoroughly completed written directives which will sufficiently enhance compliance with this issue.</p>

Recommendation	APD Action Plan (Continued)
	<p>The importance of utilizing the release of information form will also be emphasized at that training.</p> <p>Target Date: 2/1/2014</p>

Issue #7: Required Records

Observation: All IPS case files reviewed contained complete identification records, written statements of the conditions of probation, case plans setting forth behavioral and program expectations, contact logs, photographs of each IPS probationer, and documentation regarding violation behavior, positive progress, and behavioral changes.

<p>Conclusion #7A: All IPS files reviewed contained records required by statute and ACJA.</p>	
Recommendation	APD Action Plan
None	N/A

Issue #8: Initial Contacts and Orientations

Observation: IPS probation officers made initial contacts and/or conducted transition meetings within required timeframes for the vast majority of probationers reviewed. Forty of 41 (98%) in-custody probationers reviewed were contacted by the IPS officer prior to being released from jail/prison, and 29 of 31 (94%) out-of-custody probationers reviewed were contacted within 24 hours of sentencing or IPS officer notification of assignment, as required.

In addition, while most probationer orientations (92%) were conducted within required timeframes, orientations for 6 of 31 (19%) out-of-custody IPS cases were conducted outside of this timeframe.

<p>Conclusion #8A: Initial contacts and/or transition meetings were made within required timeframes for the vast majority of IPS probationers reviewed.</p>	
Recommendation	APD Action Plan
None	N/A

Conclusion #8B: Orientations for out-of-custody probationers were not always conducted within required timeframes for the IPS probationers reviewed.	
Recommendation	APD Action Plan
8B-1 Establish an effective tracking system, including appropriate oversight, to help ensure that orientations for out-of-custody IPS cases are conducted within 72 hours of sentencing or IPS officer notification of assignment.	<p>Concur – in process.</p> <p>Occasionally officers are unable to conduct orientations within 72 hours of sentencing or notification of assignment due to factors such as safety issues. While an officer may have face-to-face contact with the probationer prior to 72 hours, additional time may be required to ensure a safe setting for the orientation (e.g., the probationer is released from jail on a weekend and orientation needs to take place in the office). When this occurs, officers should document the specific reasons in an APETS entry. The next IPS Forum will include training on the importance of thorough documentation in APETS entries, which will sufficiently enhance compliance with this issue.</p> <p>Target Date: 6/25/2013</p>

Issue #9: Intensive Probation Policies and Procedures

Observation: APD has developed extensive written policies and procedures for IPS that generally comply with the ACJA requirements reviewed. However, APD lacks the required written policy for monitoring intensive probationers’ compliance with court-ordered or disclosed prescription medications. The policy should include protocols to ensure routine and timely communication between the probation officer and physician regarding compliance with dosage requirements. While APD has a policy that addresses medication monitoring, it applies to the Seriously Mentally Ill population.

Conclusion #9A: APD lacks the required written policy for medication monitoring of intensive probationers.	
Recommendation	APD Action Plan
9A-1 Develop a required written policy concerning medication monitoring for intensive probationers.	<p>Concur – in process.</p> <p>Current Policy 31.003.III.G. refers to medication monitoring as follows: Other Conditions: Monitor compliance with any other court-ordered Condition (e.g. taking medications as prescribed). Per Code the policy should be more specific, which will require a dialogue with AOC. However, it is noted that ideally probationers with prescription medicine monitoring requirements, particularly court-ordered, would not be appropriate for IPS and would be modified to a Seriously Mentally Ill caseload. Policy 31.003 will be modified to include a medical release be signed by the probationer. Additionally, the probation officer will have monthly telephonic contact with the medical provider to verify the probationer is complying with medical directives. Verification will be documented in APETS.</p> <p>Target Date: 9/1/2013</p>

Issue #10: Visual Probationer Contacts

Observation: APD probation officers are required to perform visual contacts with IPS probationers at least weekly, with at least one contact made at the probationer’s residence at least every other week. During the audit period, weekly contacts were made within required timeframes 97% of the time, and biweekly contacts were made at the probationers’ residences 96% of the time for the 71 IPS probationers reviewed. Of 3,149 weekly contacts made, only 3% were not made with the requisite frequency. Of 1,673 contacts made at probationers’ residences, only 4% were not made with the requisite frequency.

Conclusion #10A: Visual contacts were made within required timeframes for the vast majority of intensive probationers reviewed.	
Recommendation	APD Action Plan
None	N/A

Issue #11: Residence Verifications

Observation: State law requires that IPS probationers establish a residence at a place approved by the IPS team, and that the team verify the residence within one month of assignment or residence change. We reviewed 72 IPS case files and 114 probationer recorded residences (includes initial residence and subsequent moves) and found that all residences were properly approved and verified within the one-month requirement.

Conclusion #11A: IPS probationer residences reviewed were properly verified.	
Recommendation	APD Action Plan
None	N/A

Issue #12: Information Technology (IT) Control Environment

Observation: APD controls over the following areas generally followed recommended standards: 1) IT Strategic Planning / IT Investment, 2) Information Architecture, 3) Human Resource Management, 4) Information Security Policy / User Awareness, 5) Access Configuration / Segregation of Duties, 6) Access Management, 7) Patch Management, 8) Problem Management, and 9) Adult Probation Enterprise Tracking System (APETS) Application Controls.

Conclusion #12A: Through observation, limited testing, and interviews, we determined that nine key APD IT controls generally followed recommended professional standards.	
Recommendation	APD Action Plan
None	N/A

Issue #13: Law Enforcement Network and Password Management

Observation: APD uses an application called APD Online to aggregate and report data from the probationer case management system (APETS) and various other APD systems. APD Online contains sensitive law enforcement information that is not stored on the County's high-security justice and law enforcement network segment. In addition, APD Online password requirements do not meet the Criminal Justice Information Systems (CJIS) Security Policy requirements.

Conclusion #13A: Court Technology Services (CTS), the IT group supporting APD's network infrastructure, does not maintain APD Online law enforcement information within the high-security criminal justice segment of the County network.	
Recommendation	CTS Action Plan
13A-1 CTS should move APD Online into the County's high-security criminal justice network segment.	<p>Concur – completed.</p> <p>APD believed that APD Online was in fact located within <i>Zone 2</i> (the County's high-security criminal justice network segment). Immediately upon learning of the Internal Audit findings, APD and CTS worked together to ensure that APD Online was moved to Zone 2. The migration to Zone 2 has been completed and APD Online data has been removed from the Zone 3 server.</p> <p>Completion Date: 5/3/2013</p>
Conclusion #13B: APD Online does not meet CJIS Security Policy password requirements.	
Recommendation	CTS Action Plan
13B-1 CTS should implement CJIS Security Policy password requirements for APD Online.	<p>Concur – completed.</p> <p>After the initial audit finding, CTS implemented a password policy that requires APD Online users to first sign in to the County Network and validate their user ID and password before accessing APD Online. County network credentials meet or exceed CJIS Security Policy requirements. These restrictions are now in place and working well.</p> <p>Completion Date: 4/11/2013</p>

Issue #14: APD Online Change Management and Program Development

Observation: APD and CTS do not formally authorize, test, and approve changes to APD Online. CTS developers have unrestricted access to APD Online. Unauthorized, unapproved, and untested changes can create data accuracy or system availability issues.

Conclusion #14A: CTS does not have a formal change management process for authorizing, testing, and approving changes to APD Online.	
Recommendation	ADP Action Plan
14A-1 APD should work with CTS to develop a formal policy for authorizing, testing, and approving APD Online changes.	<p>Concur – completed.</p> <p>A process has been developed and formalized in order for changes to APD Online to be authorized, tested, and approved. All APD requests of CTS, including changes to APD Online, are now routed through the helpdesk and a ticket created and tracked using a program to manage software development projects called <i>Team Foundation Server</i>. This allows CTS and APD to track each request, know the status of each request, and document the changes made to APD Online. Additionally, CTS is provided with the specific employees within APD who are able to authorize/approve requests on behalf of the Department, which ensures that only approved requests are processed.</p> <p>Completion Date: 2/13/2013</p>
Recommendation	CTS Action Plan
14A-2 CTS should either limit developer direct access to APD Online (production environment) and/or implement tools to monitor developer changes.	<p>Management accepts the risk of this issue.</p> <p>While two CTS staff members do have unrestricted access to APD Online, they have Terminal Operator certification demonstrating their understanding of data integrity and the responsibilities that come with access to this data. This certification is renewed every two years which includes refresher training, testing, and updated background investigations. Additionally, the function they perform with the system does not include user account interfaces that allow data entry, as the information in APD Online comes from other sources, and the function CTS performs involves application maintenance opposed to data entry, which also reduces the likelihood of the unintentional alteration of data.</p> <p>Target Date: N/A</p>

Issue #15: IT Security Reviews

Observation: We reviewed reports and processes to verify that APD and CTS are performing critical IT security reviews. We found APD and CTS do not have formal procedures for reviewing and validating (a) accounts used to authorize network access, (b) accounts used to remotely access the network (Virtual Private Network - VPN), and (c) credentials used for data center access. We also found that 22 of 33 (66%) ADP Online administrator accounts belonged to terminated employees, and 2 of the 7 (29%) employees authorized to access ADP Online backup tapes were terminated. We reviewed software that CTS uses to manage source code and found that 1 of 10 (10%) accounts belonged to a terminated contractor. We also found that 220 of 3,508 (6%) APD computers were infected with viruses or malware.

Conclusion #15A: CTS does not consistently review critical IT security reports.	
Recommendation	CTS Action Plan
<p>15A-1 CTS should develop formal policies and procedures to periodically review:</p> <ul style="list-style-type: none"> • Active Directory, APD Online database administrator, and VPN accounts • Physical access to data centers • Back-up tape authorization • Source code management software permissions • Virus removal logs 	<p>Concur – completed or in process.</p> <ul style="list-style-type: none"> • Active Directory, APD Online database administrator, and VPN accounts – VPN accounts are addressed in CTS Procedure DS 5.4.7 <i>VPN/RAS Remote Access Account Procedure</i> that has been reviewed and will be signed by the CIO and Deputy CIO before May 10, 2013. • Physical access to data centers – The CTS Security Officer is creating a policy to address this concern and that policy will be finalized on or before July 26, 2013. • Back-up tape authorization – The CTS Operations Specialist is creating a policy to address this concern and that policy will be finalized on or before July 26, 2013. • Source code management software permissions – Source code management and software permissions are part of a procedure being drafted that governs incoming and outgoing CTS employee checklists, which includes network, database, and software access. This procedure will be finalized on or before May 30, 2013.

Recommendation	CTS Action Plan (Continued)
	<ul style="list-style-type: none"> • Virus removal logs – A review of virus logs indicate there were 220 identified viruses associated with Marcos that APD uses and are, in fact, false alerts. Additionally, according to CTS, APD only has approximately 1,640 computers, so the figure noted in issue #15 of 3,508 APD computers does not appear accurate. <p>Target Date: Identified after each item.</p>

Issue #16: Data Transfers and Reporting

Observation: APD does not use protective encryption when transmitting sensitive data from APD Online to various law enforcement agencies and an outside vendor. CTS also does not have formal procedures to ensure that transferred data or system-to-system reports are complete and accurate. Systems and reports affected include: 1) Sex Offender Density Report, 2) APETS-to-APD Online data transfer, 3) Department of Corrections-to-APD Online data transfer, and 4) APD-to-Police Department data transfers.

<p>Conclusion #16A: APD sends sensitive data to internal and external agencies without encrypting files and does not monitor the accuracy and completeness of data transmissions.</p>	
Recommendations	APD Action Plan
<p>16A-1 APD should work with CTS to ensure that sensitive data transmissions are encrypted.</p>	<p>Concur – will implement with modifications.</p> <p>Both APD and CTS agree with the recommendation, where practical. We will work towards that goal, but there may be instances where criminal justice partners do not have the necessary infrastructure or the capabilities to operate in a completely encrypted environment.</p> <p>Target Date: Completed (Ongoing)</p>

Recommendations	APD Action Plan
<p>16A-2 APD should work with CTS to develop automated job monitoring processes that promote complete and accurate data transmissions and reports.</p>	<p>Concur – will implement with modifications.</p> <p>Both APD and CTS will work together to determine the feasibility of developing job monitoring processes, with the recognition that the current hardware and software environments do pose some limitations.</p> <p>Target Date: 9/30/2013</p>

Issue #17: IT Policies and Procedures

Observation: Although APD and CTS have developed some IT policies, they have not formally documented policies and procedures for key control areas including: 1) Quality Management, 2) IT Risk Management, 3) Project Management, and 4) Disaster Recovery and Business Continuity Planning. APD also does not have formal agreements with CTS and the Administrative Office of the Courts (AOC) documenting how key applications are supported. A formal agreement between APD and AOC would strengthen controls over system operations and enhance data security.

<p>Conclusion #17A: CTS and APD have not developed formal policies and procedures for key IT processes.</p>	
Recommendation	APD Action Plan
<p>17A-1 APD should work with CTS to develop policies for quality management, IT risk management, project management, and disaster recovery planning and business continuity.</p>	<p>Concur – will implement with modifications.</p> <p>APD and CTS professionals currently meet regularly to discuss project requests, priorities of current projects and requests, progress on projects. This activity has proven satisfactory in providing technical support for APD. CTS will meet with APD and discuss this recommendation, and if it proves advantageous to formally document current practices, or develop new policies for quality management, IT risk management and project management, we will certainly endeavor to take on this task.</p> <p>The issue of disaster recovery and business continuity has been an ongoing discussion. CTS will continue to communicate and plan for disaster recovery and business continuity planning with the APD and other departments of the Judicial Branch. Currently, the Judicial Branch has a Disaster</p>

Recommendation	APD Action Plan (Continued)
	<p>Recovery (DR) site at the County Durango complex. This DR site is currently under review as the County is coordinating a higher speed communication line to the facility. CTS and the Judicial Branch are also coordinating with the Office of Enterprise Technology (County IT Department) to move our DR site from the Durango complex to the County Information Operations DR site that is currently being negotiated. CTS and APD will commit to begin discussions on disaster recovery and business continuity as it relates to APD Online and other automated systems (iCIS, iCIS NG and ICJIS data exchanges) that are currently used by APD.</p> <p>Target Date: 6/30/2014</p>
<p>Conclusion #17B: AOC and APD do not formally document their responsibilities for maintaining and managing APETS. CTS and APD also do not document their responsibilities for APD Online.</p>	
Recommendations	APD Action Plan
<p>17B-1 APD should consider working with CTS and AOC to define and document roles and responsibilities for supporting APETS.</p>	<p>Concur – will implement with modifications.</p> <p>APETS is a statewide record management system which belongs to and is administered by the Supreme Court, through the AOC, and it is listed in the Arizona Code of Judicial Administration as a state sponsored system (ACJA § 1-501). As a result and in light of operational experience since the creation of APETS, there has been sufficiently clarity in the AOC’s responsibilities as it relates to supporting APETS. Additionally, APD is a member of a larger statewide committee which approves and recommends changes to APETS giving APD the opportunity to pursue necessary fixes and enhancements. APD has specific staff members who are designated as liaisons to the AOC as it relates to APETS. Finally, the Superior Court also provides a technology strategic plan to the AOC pursuant to the Arizona Code of Judicial Administration, which provides an additional avenue for articulating Court and APD needs.</p> <p>Target Date: 6/30/2014</p>

Recommendations	APD Action Plan
<p>17B-2 APD should work with CTS to document ADP roles and responsibilities for supporting APD Online.</p>	<p>Management accepts the risk of this issue.</p> <p>Both Adult Probation and Court Technology Services are under the leadership and authority of the Presiding Judge and are two divisions in the same Judicial Branch. Therefore, the two departments have been able to reach agreement on the respective roles of the two agencies and maintain a productive and supportive relationship. Additionally, an IT Governance Committee is also present to govern the approval and acceptance of IT projects which also provides additional leadership in this area.</p> <p>Target Date: N/A</p>
Recommendation	CTS Action Plan
<p>17B-3 CTS should document its roles and responsibilities for supporting APD Online.</p>	<p>Management accepts the risk of this issue.</p> <p>Both Adult Probation and Court Technology Services are under the leadership and authority of the Presiding Judge and are two divisions in the same Judicial Branch. Therefore, the two departments have been able to reach agreement on the respective roles of the two agencies and maintain a productive and supportive relationship. Additionally, an IT Governance Committee is also present to govern the approval and acceptance of IT projects which also provides additional leadership in this area.</p> <p>Target Date: N/A</p>

**Audit Team
Members**

Deputy County Auditor Eve Murillo, CPA, MBA, CFE, ITIL, CLEA
Deputy County Auditor Richard Chard, CPA
Audit Supervisor Carla Harris, CPA, CIA, CFE
Senior Auditor Kimmie Wong, MPA, CLEA
Senior Auditor Jenny Eng, CIA, CGAP
Senior Auditor Stacy Aberilla, MPA
Associate Auditor Ryan Barber, BS

**IT Audit Team
Members**

IT Audit Supervisor Patra Carroll, MSIM, CPA, CIA, ITIL, CITP
Senior IT Auditor Susan Adams, MBA, CISA, ITIL, CLEA
Senior IT Auditor Jacob Pacini, MSIM
KPMG LLP

This report is intended primarily for the information and use of the County Board of Supervisors, County leadership, and other County stakeholders. However, this report is a matter of public record, and its distribution is not limited.

We have reviewed this information with the APD Chief Probation Officer and CTS Chief Information Officer. The Action Plan was approved by Norman Davis, Superior Court Presiding Judge, and Barbara Broderick, Chief Probation Officer, on June 21, 2013. If you have any questions about this report, please contact Eve Murillo, Deputy County Auditor, at 506-7245.