

Item 30

# Travis County Commissioners Court Agenda Request

**Meeting Date:** September 11, 2012

**Prepared By/Phone Number:** Deborah Trotter 854-7069

**Elected/Appointed Official/Dept. Head:** Estela P. Medina 854-7069

**Commissioners Court Sponsor:** Judge Biscoe

## **AGENDA LANGUAGE:**

Consider and take appropriate action on the Integrated Child Support System Cooperative agreement between Travis County and the Attorney General of the State of Texas.

## **BACKGROUND/SUMMARY OF REQUEST AND ATTACHMENTS:**

This contract is a renewal of a current contract in effect since 7/1/08 with the Texas Attorney General whereby the County through a Standing Judicial Order designates all new divorces in which child support is ordered since 7/1/09 as Title IV-D cases and assigns the Domestic Relations Office the responsibility of monitoring, enforcing, and modifying said orders should the need arise. The renewal contract period is 9/1/12 through 8/31/14.

## **STAFF RECOMMENDATIONS:**

The Travis County Juvenile Probation Department respectfully recommends approval of the Travis County Integrated Child Support System Cooperative Agreement.”

## **ISSUES AND OPPORTUNITIES:**

## **FISCAL IMPACT AND SOURCE OF FUNDING:**

## **REQUIRED AUTHORIZATIONS:**

**AGENDA REQUEST DEADLINE:** All agenda requests and supporting materials must be submitted as a pdf to Cheryl Aker in the County Judge's office, [Cheryl.Aker@co.travis.tx.us](mailto:Cheryl.Aker@co.travis.tx.us) by Tuesdays at 5:00 p.m. for the next week's meeting.



# TRAVIS COUNTY JUVENILE PROBATION DEPARTMENT

ESTELA P. MEDINA  
Chief Juvenile Probation Officer

ADMINISTRATIVE SERVICES  
COURT SERVICES  
DETENTION SERVICES  
PROBATION SERVICES  
RESIDENTIAL SERVICES  
SUBSTANCE ABUSE SERVICES  
DOMESTIC RELATIONS OFFICE

## MEMORANDUM

**TO:** The Honorable Samuel T. Biscoe, County Judge  
The Honorable Ron Davis, Commissioner, Precinct 1  
The Honorable Sarah Eckhardt, Commissioner, Precinct 2  
The Honorable Karen Huber, Commissioner, Precinct 3  
The Honorable Margaret J. Gomez, Commissioner, Precinct 4

**FROM:**   
Estela P. Medina  
Chief Juvenile Probation Officer

**SUBJECT:** Travis County Integrated Child Support System Cooperative Agreement

**DATE:** September 4, 2012

The Travis County Juvenile Probation Department is respectfully requesting that the attached Cooperative Agreement be placed before the Commissioner's Court for approval. The request is asking for approval of the Cooperative Agreement of the Travis County Integrated Child Support System between the Office of the Attorney General, and Travis County. This agreement was first approved by the Court in July, 2009.

The Cooperative Agreement has also been previously reviewed by the Travis County Juvenile Board during a regularly scheduled meeting on August 29, 2012.

Thank you for your consideration and please advise of any additional information you may need.

Thank you.

**CC:** Judge Darlene Byrne, 126<sup>th</sup> District Court  
Aerin Toussaint, PBO  
Scot Doyal, DRO





**TRAVIS COUNTY  
INTEGRATED CHILD SUPPORT SYSTEM  
COOPERATIVE AGREEMENT**

**CONTRACT NO. 13-C0105**

This Agreement is entered into by and between the OFFICE OF THE ATTORNEY GENERAL ("OAG"), as Title IV-D Agency for the State of Texas, for and on behalf of its Child Support Enforcement Division ("Division") and Travis COUNTY of the State of Texas ("County") under the authority of Section 231.002 of the Texas Family Code.

WHEREAS, pursuant to Title IV, Part D of the federal Social Security Act and Chapter 231 of the Texas Family Code, the OAG has been designated as the Title IV-D agency for the State of Texas; and

WHEREAS, the OAG as the designated Title IV-D agency has been delegated responsibility for developing and administering a statewide integrated system for child support and medical support enforcement ("Texas ICSS"); and

WHEREAS, the OAG and the County desire to enter into an agreement for the County to provide the services enumerated herein;

NOW, in furtherance of the aforesaid objectives and in consideration of the mutual understanding and agreements hereinafter set forth, OAG and County agree as follows:

**1. PURPOSE**

The OAG and County shall cooperate to provide comprehensive, effective, and efficient child support enforcement services to:

- 1.1. record, monitor and enforce all County child support orders entered in the Qualifying CSE Caseload;
- 1.2. utilize the OAG computer system for delinquency monitoring, billing, and other enforcement techniques to ensure the payment of current child support and medical support to custodial parents in the Qualifying CSE Caseload;
- 1.3. incorporate existing enforcement resources into the automated enforcement process to obtain maximum benefit from federal funding;
- 1.4. delineate requirements for implementing an effective and compliant County run integrated child support enforcement office;

- 1.5. ensure parties in the cases in the Qualifying CSE Caseload receive quality customer service;
- 1.6. ensure compliance by County with all federal and state laws and regulations governing IV-D child support and medical support;
- 1.7. delineate OAG processes to support County efforts; and
- 1.8. ensure seamless transition of services upon termination of this Agreement.

## 2. **DEFINITIONS**

For the purposes of this Agreement, the terms listed below shall have the following meanings:

- 2.1. "Allowable Costs" shall be the actual amount of costs incurred that qualify for reimbursement under the federal financial participation provisions of Part D, Title IV of the federal Social Security Act (42 U.S.C. §§ 651 *et seq.*) and Office of Management and Budget Circular A-87, "Cost Principles for State and Local Governments", published by the Executive Office of the President of the United States of America.
- 2.2. "County Participants" shall mean the various County departments (excluding the Community Supervision Unit) which either perform IV-D Program Activities or support the performance of IV-D Program Activities by providing administrative support services such as facilities management or procurement assistance. County costs associated with the Community Supervision Unit are covered under a separate contract.
- 2.3. "County Personnel" shall mean the personnel provided by County to perform work in the County's enforcement office, and whose time on the job is dedicated in whole or in part to IV-D Program Activities. Such personnel may be either county employees or staff provided by private contractors, as County deems appropriate.
- 2.4. "Direct Costs" shall be defined as that term is defined by the federal Office of Management and Budget Circular A-87, "Cost Principles for State and Local Governments", published by the Executive Office of the President of the United States of America.
- 2.5. "Division" shall mean the Child Support Division of the OAG.
- 2.6. "ICSS" shall mean the Integrated Child Support System, a cooperative effort established by the OAG pursuant to Chapter 231 of the Texas Family Code.
- 2.7. "Indirect Costs" shall be defined as that term is defined by the federal Office of Management and Budget Circular A-87, "Cost Principles for State and Local Governments", published by the Executive Office of the President of the United States of America.
- 2.8. "IV-D Program Activities" shall be those activities exclusively devoted to fulfilling the requirements, duties, and obligations of a child support enforcement office pursuant to state and federal law.
- 2.9. "OAG Computer System" shall mean the Texas Child Support Enforcement System

(TXCSES), a federally certified case management system for the IV-D program.

- 2.10. "Qualifying CSE Caseload" shall mean all Child Support orders deemed to have made an application for Title IV-D Child Support services by the County local rule and entered subsequent to the effective date of the local rule as defined in the Texas Rules of Civil Procedure 3a, and deemed to be a IV-D case by way of the local rule.
- 2.11. "Title IV-D agency" shall have the meaning defined in Section 101.033 of the Texas Family Code.
- 2.12. "Title IV-D case" shall have the meaning defined in Section 101.034 of the Texas Family Code.

### **3. TERM OF AGREEMENT**

This Agreement is effective on September 1, 2012 and, unless sooner terminated as provided herein, shall terminate August 31, 2014.

### **4. OAG RESPONSIBILITIES**

The OAG will:

- 4.1. Purchase, install, and maintain using OAG funds, computer hardware and related equipment which the OAG and County deem necessary (not to exceed the standard OAG hardware configuration) for County Participants to process the qualifying CSE caseload using the OAG computer system;
- 4.2. Purchase, install, and maintain computer software and upgrades to OAG procured software which OAG and County deem necessary (not to exceed the standard OAG software configurations) for County Participants to process the qualifying CSE caseload using the OAG computer system;
- 4.3. Provide access to County Personnel for the OAG computer system consistent with OAG software license agreements and OAG computer system capacity and capability;
- 4.4. Provide, at OAG expense and discretion, training to County Personnel in the use of the OAG computer system and its component hardware and software. When OAG determines that it is feasible, training will be conducted locally;
- 4.5. Provide through OAG region and office management specific technical assistance, training, procedural and policy support as needed to assist the County Participants with ongoing operational issues. If the Regional Administrator requests that the County attorneys who perform services under this Agreement attend state-wide training conducted by the OAG for Assistant Attorneys General, or that County Participants attend an OAG Statewide Managers' Meeting or Field Managers' Meeting, or if OAG State, Regional or Office level management requests that County Participants attend OAG training relating to the services being performed by County under this Agreement, the cost for such travel will be separately reimbursed. The cost for such travel is not included in the per child support order fee set forth in the

Reimbursement of Certain Allowable Costs Section below. The OAG will reimburse such cost subject to the rates specified for travel by its own classified employees, for the expenses approved by the OAG that are allowable for reimbursement in the State of Texas Travel Allowance Guide. Any claim for such travel reimbursement by County shall include adequate supporting documentation as prescribed in the State of Texas Travel Allowance Guide. County and OAG agree that claims for such travel reimbursement may be submitted directly to the OAG by the individual traveler and that the OAG may make payment for such travel reimbursement directly to the individual traveler. Any claim submitted by an individual traveler must contain the traveler's full name, mailing address, contact phone number, Social Security Number and OAG Contract Number.

- 4.6. Make available applicable federal, state, and local rules and procedures to County Personnel and provide updates as appropriate and consistent with OAG policy and field operations;
- 4.7. Be responsible for those IV-D cases not included in the Qualifying CSE Caseload as that term is defined in this Agreement; and
- 4.8. Provide a statement of intent to renew to the County on or before April 1, 2014. If the OAG intends to renew, not later than June 1, 2014, the OAG will provide the County with a proposed child support order fee together with the component annual cost elements; which proposed order fee will be based upon actual OAG state appropriation year 2013 expenditures and encumbrances with an as of date no earlier than May 1, 2014.

## 5. COUNTY RESPONSIBILITIES

The County will, pursuant to funds provided by Commissioner's Court:

- 5.1. Provide physical facilities for County Participants as necessary to timely process the Qualifying CSE Caseload and to accommodate information system needs, including but not limited to related utility services and physical support;
- 5.2. Provide County Personnel as necessary to effectively and efficiently administer, including administrative and judicial enforcement of, the Qualifying CSE Caseload in compliance with federal and OAG performance measures and requirements and federal Data Reliability standards. Such staff may be either county employees or private contractors, as County deems appropriate, but subject to the Subcontracting Section in the General Requirements Section below;
- 5.3. Make every attempt to ensure consistent information resource (IR) personnel support exists for the timely completion of OAG IR projects;
- 5.4. Comply with federal and (as specified by the OAG) OAG requirements and procedures regarding case initiation, record retention, reporting, confidentiality, case processing, administrative enforcement, judicial enforcement and money handling. County shall use the TXCSES "Legal Diary" that is used to populate the Automated Local Printing System. The County may use County authored forms unless the use of such form(s) would: cause the OAG not to be in compliance with federal and state laws, rules and regulations governing ICSS and child support enforcement; result in the loss of historical data or cause the County not to meet

any of the minimum performance standards set forth in the Performance Evaluation Standards subsection below. Provided however, that when the OAG implements its document management system the County must then use OAG authored forms. The County may request that the OAG approve County local variances to the OAG authored forms. The OAG will expedite the review of such requests. The review will be conducted by personnel specifically appointed, by the Director, Child Support Division, to review County local variance requests. The OAG will keep the County informed of the planned implementation date for the OAG document management system and will provide the County with a minimum of ninety (90) calendar days prior written notice of the migration date(s) for the document management system;

- 5.5. Record all support orders in the Qualifying CSE Caseload in the OAG computer system;
- 5.6. Utilize the OAG computer system to monitor and enforce all orders in the Qualifying CSE Caseload;
- 5.7. Within statutory requirements in conjunction with section 4.3 above, modify and maintain the existing County computer systems to effectively and efficiently administer the Qualifying CSE Caseload and integrate with the OAG computer system;
- 5.8. Provide office: furniture, equipment, and supplies as necessary for County Personnel to perform the duties described herein;
- 5.9. To the extent necessary to fulfill its obligations under this Agreement, maintain County procured equipment compatibility with the OAG computer system and OAG procured computer equipment, to include computer hardware and related equipment upgrades. OAG will provide County with as much notice as possible of intended OAG computer system and OAG procured computer equipment upgrades.
- 5.10. Ensure that, when requested by the Regional Administrator or the Senior Regional Attorney, County attorneys who perform services under this Agreement attend state-wide training conducted by the OAG for Assistant Attorneys General, and that County Participants attend OAG Statewide Managers' Meetings or Field Managers' Meetings, and also ensure that, when requested by OAG State, Regional or Office level management, County Participants attend OAG training relating to the services being performed by County under this Agreement.

## 6. REIMBURSEMENT OF CERTAIN ALLOWABLE COSTS

- 6.1. Reimbursement. The OAG shall reimburse the County for the federal share of the County's Agreement associated allowable cost subject to the limitations set forth in this Agreement. Federal share means the portion of the County's Agreement associated allowable cost that the federal Office of Child Support Enforcement reimburses the state as federal financial participation under Title IV-D; for purpose of reference only the federal share on the effective date of this Agreement is 66%. The Cost Principles for "State and Local Governments" as defined in OMB Circular A-87 shall apply to costs reimbursed under this Agreement. The County and OAG agree that for the purposes of this Agreement all of the County's Agreement associated allowable costs for any given calendar month is equal to the obligated caseload that was in existence on the first day of that month multiplied by a per child support order fee of

\$17.70. For the purposes of this section the obligated caseload is defined as:

“All cases with sufficient information on the OAG automated child support system to be counted as an obligated case on the OAG’s monthly Goals and Production Report – BMI100 Goals and Production.”

Thus: (Obligated Caseload) X (\$17.70) X (Federal Share) = OAG Reimbursement Amount.

The child support order fee was determined by first identifying the direct costs of an equivalent Child Support Division Field Office and the indirect costs of OAG attributable to the support of that office (which indirect costs would not also be provided in kind to the County enforcement office) based upon actual OAG state appropriation year 2012 expenditures and encumbrances as of May 18, 2012.

6.2. Incentive Payments for Exceeding Quality and Efficiency Standards. If County qualifies for an incentive payment (see the Quality and Efficiency Standards Subsection of the Performance Measurement Section below) either thirty cents (\$0.30), thirty-five cents (\$0.35) or forty cents (\$0.40), depending upon the incentive amount qualified for, shall be added to the per child support order fee set forth above for the calendar month that the County qualified for the incentive payment.

6.3. Reimbursement Process.

6.3.1. OAG shall determine the monthly fee based on the obligated caseload in existence on the first day of the month and the results of the Quality and Efficiency Monitoring.

6.3.2. OAG shall forward a Quality and Efficiency Report and Reimbursement Invoice to the County for review and approval.

6.3.3. If the County approves the Quality and Efficiency Report and Reimbursement Invoice, the County signs the Invoice and returns it to OAG within ten (10) County work days. County’s signature constitutes approval of the Invoice and certification that all services provided during the period covered by the Invoice are included on the Invoice. The OAG shall process the invoice for payment in accordance with the state procedures for issuing state payments and the Texas Prompt Payment Act.

County shall either submit the invoice via US Mail to:

Karla McDougal, Contract Manager  
Mail Code: 062  
Office of the Attorney General  
P.O. Box 12017  
Austin, Texas 78711-2017

via facsimile to: (512) 460-6980 or (512) 460-6618

or via email to: [karla.mcdougal@texasattorneygeneral.gov](mailto:karla.mcdougal@texasattorneygeneral.gov)

6.3.4. If County does not approve the Quality and Efficiency Report and Reimbursement Invoice, it shall respond to the OAG via email within ten (10) County working days of receipt, detailing



the basis of any disputed item along with supporting documentation. The OAG shall review disputed items. If the dispute is resolved in the County's favor, the OAG shall make payment in the amount requested by County. If the dispute is not resolved in the County's favor, the OAG shall make payment in accordance with the Invoice originally sent to the County and forward a letter of explanation to the County.

6.4. Limitations on Reimbursement.

- 6.4.1. Non-Receipt of Federal Share. The OAG is liable to the County for payment of the federal share of reimbursement to the extent that the OAG receives the federal share. If the federal share is received by the OAG and that amount or any part of it is later disallowed by the federal government, the County official to whom payment was made shall return the amount disallowed to the OAG not later than the thirtieth (30th) day after the date on which notice to return the disallowed amount was given by the OAG.
- 6.4.2. No Reimbursement For Costs Incurred Prior to Agreement. The OAG shall not be liable to reimburse the County for allowable costs pursuant to this Agreement when such costs were incurred prior to the commencement of this Agreement or are incurred after termination of this Agreement.
- 6.4.3. Timing of Requests for Reimbursement. The OAG may decline to reimburse County for any services not properly billed to the OAG within the next three billing cycles immediately following the month in which the County provided the services.
- 6.4.4. No Reimbursement When Non-Compliance with Inventory Control Requests or Denial of Access to Records. The OAG shall not be liable to reimburse the County for allowable costs pursuant to this Agreement from the date that any personnel employed or retained by the County subject to this Agreement fail to comply with OAG inventory control requests or fail to grant immediate access to all books, records and equipment subject to this Agreement to representatives of the United States Department of Health and Human Services ("HHS"), the Comptroller General of the United States, the OAG, the State Auditor, or their agents and representatives for purposes of inspecting, monitoring, auditing, evaluating, or copying such items. The OAG shall continue to have no obligation to reimburse the County for such allowable costs until said personnel comply with the inventory control requests and/or grant access to such books, records and equipment.
- 6.4.5. Reimbursement Subject to Federal Approval. It is expressly understood and agreed by the parties hereto that any and all of the OAG's obligations hereunder are contingent upon the existence of a State Plan for Child Support Enforcement approved by the federal Office of Child Support Enforcement providing for the statewide program of child support enforcement pursuant to the Social Security Act, and on the availability of federal financial participation for the activities described herein. In the event that the State Plan should be disapproved, or the availability of federal financial participation is otherwise terminated, the OAG shall discontinue payment hereunder and notify the County within ten (10) days of such fact in writing, except that the OAG shall reimburse the County for any costs incurred pursuant to this Agreement for which the OAG receives money from the federal Office of Child Support Enforcement.

- 6.4.6. County Refund of Overpayments. The County shall refund to the OAG within thirty (30) calendar days any sum of money which has been paid to the County which the OAG and the County agree has resulted in an overpayment to the County, provided that such sums may be offset and deducted from any amount owing but unpaid to the County.
- 6.4.7. Withhold of Funds Upon Loss, Damage, or Theft of Equipment. Upon the loss, damage, or theft of any OAG provided equipment, the OAG may withhold an amount equal to the fair market value of the equipment until final resolution of County liability (and any required payment to OAG, if any) under the "Property Management, Accountability and Maintenance" section of this Agreement.

## 7. **FEDERAL INCENTIVE PAYMENTS**

- 7.1. County May Qualify for Incentive Payments. In addition to the reimbursements specified in the "Reimbursement of Certain Allowable Costs" section of this Agreement, federal law provides that eligible political subdivisions may share in federal incentive revenues. County shall participate in Texas' earned incentives in the following incentive measures: Collections on Current Support, Collections on Arrears and Collections to Expense Ratio. County's eligible share shall be calculated in a manner consistent with the way OCSE calculates Texas' share of federal incentives. In addition, County share shall be determined in the same proportion that County collections constitute part of the federally defined collections base and that OAG field offices' costs constitute part of the overall annual costs of the Texas IV-D program. The proportion of field offices' costs to overall annual IV-D program costs will be computed based on actual expenditure and encumbrance data for the state appropriations year that encompasses eleven (11) months of the federal fiscal year for which federal incentives were awarded to the state. Upon the United States Office of Child Support Enforcement providing OAG with an accounting of Texas' share of the national performance incentives pool, and completing payment of any incentives due OAG, OAG will calculate County's proportionate share of performance incentives and make payment to County of any performance incentives due County. The requirements imposed upon OAG by the "Federal Incentive Payments" section and its subsections shall survive the termination of this Agreement until such time that OAG has fulfilled its obligations under the aforesaid "Federal Incentive Payments" section and its subsections.
- 7.2. Conditions for Earning Federal Incentive Payments. County must be performing satisfactorily at the end of the State fiscal year to be eligible to share in any federal incentives realized by OAG for the Federal fiscal year that encompasses eleven (11) months of that State fiscal year (see the "Remedies for Non-Performance" section below). The State fiscal year runs from September through the following August. The Federal fiscal year runs from October through the following September.
- 7.3. Federally defined performance incentive measures. To the extent that County performs each of the following incentive measures County shall receive its ratio share of incentives. County at the inception of this Agreement does not establish parentage or support orders and therefore is not eligible to share in the first two incentive measures listed:

Parentage Established Percentage  
Cases with Support Orders

Collections on Current Support  
Collections on Arrears  
Collections to Expense Ratio

Attachment One to this Agreement provides an example illustrating the allocation methodology. The example presented as Attachment One is offered for purposes of illustration only and is not intended to represent an agreement to pay to the County the dollar amounts listed in the Attachment.

- 7.4. **Requirement to Maintain a Base Year Level of Expenditures.** County must expend the full amount of incentive payments received under this Agreement to supplement and not supplant other funds used by the County to carry out the services being provided under this Agreement. County expenditures may not be reduced as a result of the receipt and reinvestment of incentive payments. A base year level of county expenditures has been identified to determine if incentive payments are used to supplement rather than supplant other funds used by the County to carry out the services being provided under this Agreement. The base year is September 1, 2006 through August 31, 2007. The base year level of expenditures is Two Hundred Seventy-Three Thousand Five Hundred Ninety-Five Dollars and no/100 (\$273,595.00). This base year level of expenditures must be maintained in future years. Incentive payments received under this Agreement must be used in addition to and not in lieu of this base amount.
- 7.5. **Audit.** The listing of audit requirements in this particular subsection is not intended to and do not exclude the applicability of the audit requirements set forth in the "Audit Provisions" section below. Rather the requirements of this subsection are cumulative and in addition to the requirements of the "Audit Provisions" section below. County shall maintain and retain for a period of three (3) years after the termination of this Agreement, or until full and final resolution of all audit or litigation matters which arise before the expiration of the three (3) year period, whichever time period is longer, such records as are necessary to fully disclose that incentive payments received under this Agreement were used to supplement and not supplant the base year level of expenditures. If incentive payments are disallowed as a result of an audit finding contained in an audit (by the County's independent auditor, the OAG, the State auditor, the US Department of Health and Human Services, the Comptroller General of the United States, or any of their duly authorized representatives) that the County has used the incentive payments to supplant and not to supplement the base year level of expenditures, then the County shall refund to OAG the amount supplanted within thirty (30) calendar days of the date of the written OAG request for refund; provided further that such amounts may be offset and deducted from any funds payable under this Agreement.
- 7.6. **Revision of Incentive Payment Methodology.** If the federal incentive payment methodology is changed during the term of this Agreement, OAG and County will execute an amendment to conform to the new methodology.

8. **PERFORMANCE MEASUREMENT AND CHALLENGE GOALS**

- 8.1. **Performance Requirements.** The County shall comply with all federal and state laws, rules and regulations governing ICSS and child support enforcement including, but not limited to, Chapter 231 of the Texas Family Code and Title IV-D of the federal Social Security Act and

(as specified by the OAG) the policies and procedures of the OAG for implementing those state and federal requirements. The County agrees to allow the OAG to have unannounced access to and to monitor the County IV-D office and to observe the operation of and to perform investigations, audits and reviews of the operation and records of the office as deemed necessary by the OAG to assure compliance with federal and state requirements, OAG policies and procedures or other written OAG requirements. The County agrees to facilitate OAG reporting of relevant monitoring, enforcement, and customer service actions by appropriate recording of activities and information on the OAG automated child support system ("TXCSES") or (as may be required by the OAG) by preparing reports of such relevant information as may be recorded on the County automated systems. The County agrees to work with the OAG Regional Administrator on a regular basis to evaluate the month-to-month performance by the County of its obligations under this Agreement.

8.2. Performance Evaluation Standards. The County agrees that, at a minimum, it shall perform its obligations under this Agreement according to the following standards:

8.2.1. Federal Data Reliability Standards. County shall meet the ninety-five percent (95%) efficiency rate for the completeness, reliability and accuracy of the data that underlie Lines 1, 24, 25, 28 and 29 of Form OCSE 157.

8.2.2. Customer Service Standards. County shall track and provide documentation regarding all inquiries received. These activities shall be tracked by using the Case Correspondence screen on TXCSES. All inquiries shall include a statement of the inquiry, a statement of the action taken to assist the customer, a statement of any follow up action and final result, the name of the person handling the inquiry, the name of the person making the inquiry, OAG case number and/or court cause number, NCP name, CP name, and date of inquiry. County shall perform Customer Service according to the following time-lines:

- respond to written inquiries within ten (10) County work days,
- respond to e-mail inquiries within ten (10) County work days,
- take action on information received within three (3) County work days,
- document case record of action or information received at time of receipt,
- follow up to a telephone inquiry within three (3) County work days,
- complete any necessary research within fifteen (15) County work days,
- return phone calls within two (2) County work days,
- see an in-office customer the same day, and
- schedule any request for an appointment within three (3) County work days of request.

8.2.3. Public Official Inquiry Standards County shall process Public Official inquiries in accordance with the following standards. County may choose to respond to the inquiry itself or have the OAG Public Official Services Section ("POS") respond. When the County chooses to have the POS respond County must notify POS immediately upon receipt of either a telephonic or written inquiry. County must provide POS with the case number, name of the person calling, and on whose behalf the person was calling. In case of a written inquiry County must fax the written inquiry to POS immediately upon receipt. County shall assist POS with resolving the inquiry. When County chooses to respond itself, County must, in consultation with POS, respond to a written inquiry within five (5) County work days and a telephone inquiry the same day if possible. Immediately

after responding, County must notify the POS supervisor of the inquiry received and its resolution. County must respond to any POS tasking within two County work days of the date of the e-mail. County must notify POS supervisor of any public official inquiry relating to a case that is not pending in the County office.

- 8.2.4. Percentage of Collections on Current Support Due. The standard for this category shall be collecting annually at least the percentage of current support due designated by the OAG as the statewide minimum standard for OAG field offices. The OAG Contract Manager shall inform the County office of the amount designated as the statewide minimum standard on or before October 31 of the federal fiscal year.
- 8.2.5. Percentage of Cases with Collections on Arrears. The standard for this category shall be achieving annually at least the percentage of cases with collections on arrears designated by the OAG as the statewide minimum standard for OAG field offices. The OAG Contract Manager shall inform the County office of the amount designated as the statewide minimum standard on or before October 31 of the federal fiscal year.
- 8.2.6. Quality and Efficiency Standards. The Quality and Efficiency Standards are set forth in the table below. County may qualify to receive an incentive payment for exceeding these minimum Quality and Efficiency Standards. In order to qualify to receive an incentive payment the County must not be in an unsatisfactory performance status (See the "Remedies for Non-Performance" section below). In order to receive a thirty cent (\$0.30) incentive payment the County must meet or exceed the specified exceptional standard for at least eight of the Quality and Efficiency measurements and achieve at least the minimum standard specified for all measurements. In order to receive a thirty-five cent (\$0.35) incentive payment the County must meet or exceed the specified exceptional standard for at least ten of the Quality and Efficiency measurements and achieve at least the minimum standard specified for all measures. In order to qualify for a forty cent (\$0.40) incentive payment the County must meet or exceed the specified exceptional standard for all measurements and achieve at least the minimum standard specified for all measurements.

If in any given month a measurement sample contains less than thirty-five (35) cases, the score for that measurement will be assumed to be exceptional, regardless of the actual score, pending results of an annual evaluation of the measurement. At the end of the fiscal year (August), an annual score will be calculated for each measurement with less than thirty-five cases (35) during any month of the fiscal year. If the annual score does not meet the exceptional standards, any payments made during the fiscal year for assumed exceptional performance will be deducted from the August invoice.

- 8.2.6.1. Statistical Sampling. The OAG may use statistical sampling, as described in Attachment Two, and generalize from sample results wherever appropriate to evaluate compliance and achievement of performance standards in order to support payment of incentives and/or assertion of remedies. For the purposes of this section, high volume performance requirements where evaluation of all relevant cases or case activities is not cost-effective or feasible shall be deemed appropriate for statistical sampling.

<b><u>MEASUREMENT</u></b>	<b><u>CRITERIA</u></b>	<b><u>MINIMUM STANDARD</u></b>	<b><u>EXCEPTIONAL STANDARD</u></b>
<b><u>CASE INITIATION AND ORDER ENTRY</u></b>	All relevant case and member data updated and order information updated within 20 business days of case opening	Ninety-five percent (95%) of all cases opened during the month reviewed.	Ninety-five percent (95%) of all cases updated and order information updated within 14 business days of case opening.
<b><u>CASE TRANSFER</u></b>	Transfer case to appropriate OAG field office within 15 business days of receipt of "Case Type Change" morning mail message.  Exception: If pending legal action exists when case type changes, case should be transferred to appropriate OAG field office within 10 business days of resolution of legal action.	Ninety percent (90%) of all cases that should have been transferred during the month reviewed.	Ninety-one percent (91%) of all cases that should have been transferred during the month reviewed.
<b><u>CASE CLOSURE</u></b>	<ul style="list-style-type: none"> <li>▪ Case closure reason code correct</li> <li>▪ Documentation in case folder and on system to verify closure reason</li> <li>▪ Wait mandatory time before closing case</li> </ul>	Ninety-five percent (95%) of all cases that were closed during the month reviewed.	Ninety-six percent (96%) of all cases that were closed during the month reviewed.
<b><u>REVIEW AND ADJUSTMENT</u></b>	Within 180 calendar days of request for review OR of locating the non-requesting party (whichever occurs later), conduct review and adjust order (by requesting modification), or determine that order should not be adjusted. Provide all parties with modified order within 14 business days after order entered OR notice	Ninety-five percent (95%) of all cases where parties should have been provided with a modified order or notified that order will not be adjusted during the month reviewed.	Ninety-six percent (96%) of all cases where parties should have been provided with a modified order or notified that order will not be adjusted during the month reviewed.

<b><u>MEASUREMENT</u></b>	<b><u>CRITERIA</u></b>	<b><u>MINIMUM STANDARD</u></b>	<b><u>EXCEPTIONAL STANDARD</u></b>
	that order will not be adjusted within 14 business days of determination.		
<b><u>LOCATE</u></b>	All appropriate locate resources utilized within 75 calendar days.	Ninety-five percent (95%) of cases where locate resources should have been utilized during the month reviewed.	Ninety-six percent (96%) of all cases where locate resources should have been utilized during the month reviewed.
<b><u>ADMINISTRATIVE INCOME WITHHOLDING</u></b>	IWO issued within 2 business days of employment verification.	Ninety-five percent (95%) of all cases with new employment information during the month reviewed.	Ninety-six percent (96%) of all cases with new employment information during the month reviewed.
<b><u>ENFORCEMENT</u></b>	Administrative Enforcement action taken within 30 calendar days of delinquency date or verified locate, whichever is later. OR Service completed (or unsuccessful service attempts documented to show diligent effort) within 60 calendar days of delinquency date or verified locate, whichever is later.  "Delinquency Date" as used in this cell means 30 days after a missed payment.	Ninety-five percent (95%) of all cases where enforcement action should have been taken or where service should have been completed during the month reviewed.	Ninety-six percent (96%) of all cases where enforcement action should have been taken or where service should have been completed during the month reviewed.
<b><u>EXPEDITED PROCESSES – 6 MONTHS</u></b>	Legal actions completed within six months from the time of successful service on all parties	Seventy-five percent (75%) of legal actions completed within six months from the time of successful service on all parties.	Seventy-six percent (76%) of legal actions completed within six months from the time of successful service on all parties.
<b><u>EXPEDITED PROCESSES – 12 MONTHS</u></b>	Legal actions completed within twelve months from the time of successful service on all	Ninety percent (90%) of legal actions completed within twelve months year from the time of	Ninety-one percent (91%) of legal actions completed within twelve months from the

<b><u>MEASUREMENT</u></b>	<b><u>CRITERIA</u></b>	<b><u>MINIMUM STANDARD</u></b>	<b><u>EXCEPTIONAL STANDARD</u></b>
	parties	successful service on all parties.	time of successful service on all parties.
<b><u>AFTER COURT ORDER ENTRY</u></b>	All subsequent orders entered into TXCSES within 7 business days of the final hearing.	Ninety percent (90%) of all subsequent orders entered into TXCSES during the month reviewed.	Ninety-one percent (91%) of all subsequent orders entered into TXCSES during the month reviewed.
<b><u>SUCCESSFUL DISPOSITION</u></b>	Legal filings successfully disposed within one year of filing.  “Successful disposition” for this purpose is defined as a final, temporary or interim order obtained or a capias issued. A nonsuit or dismissal without prejudice is not considered a successful disposition.	Seventy-five percent (75%) of all filings successfully disposed within one year of filing.	Eighty percent (80%) of all filings successfully disposed within one year of filing.
<b><u>SERVICE RATE</u></b>	Successful service of process on all parties within six months of filing.  Successful service can be via personal service, substitute service, waiver of service or personal appearance.	Seventy-five percent (75%) of all service of process issued.	Eighty percent (80%) of all service of process issued.

8.3. **Challenge Goals.** The OAG challenges its field offices, in their pursuit of excellence, to continually improve their performance, which in turn improves the overall performance of the Program and service to the children of Texas. The County agrees to participate in this challenge and use its best efforts to meet or exceed each of the goals as described below.

8.3.1. **Annual Disbursement Goal.** The standard for this category shall be disbursement of at least the amount designated by the Regional Administrator at the beginning of each state fiscal year as the county office’s annual disbursement goal. The Regional Administrator shall inform the county office of the amount designated as its annual disbursement goal on or before September 30 of the state fiscal year. The designated percentage shall be calculated by OAG Field Operations using a standardized formula.



8.3.2. Annual Medical Support Disbursement Goal. The standard for this category shall be disbursement of at least the amount designated by the Regional Administrator at the beginning of each state fiscal year as the County office's annual medical support disbursement goal. The Regional Administrator shall inform the County office of the amount designated as its annual medical support disbursement goal on or before September 30 of the state fiscal year. The designated percentage shall be calculated by OAG Field Operations using a standardized formula.

8.4. Remedies for Non-Performance.

8.4.1. Failure by the County office to meet any of the minimum performance evaluation standards in the "Performance Evaluation Standards" section and its subsections above or any of the requirements of this Agreement, except the annual challenge goals in the "Annual Challenge Goals" section and its subsections above, may result in a finding of unsatisfactory performance. County must be performing satisfactorily at the end of the State fiscal year to be eligible to share in any federal incentives realized by OAG for the Federal fiscal year that encompasses eleven (11) months of that State fiscal year. Any finding of unsatisfactory performance, either by the OAG Contract Manager or the Regional Administrator, will be communicated to the County in writing by the OAG Contract Manager. The OAG Contract Manager will review the written finding of unsatisfactory performance and, in consultation with the County and the Regional Administrator, determine the validity of the finding. The OAG Contract Manager will communicate in writing the results of the review to the County and the Regional Administrator.

8.4.2. If the finding of unsatisfactory performance is validated, the County shall be requested to provide the OAG Contract Manager with a corrective action plan. A corrective action plan, acceptable to the OAG Contract Manager, must be provided within a reasonable time period as specified by the OAG Contract Manager.

8.4.3. If the County does not return to satisfactory status within forty-five (45) calendar days after receiving notice that an unsatisfactory performance finding has been validated, then the OAG may withhold payments due to County under this Agreement until the County is once again performing satisfactorily. If the County has not either returned to satisfactory status within sixty (60) calendar days after receiving notice that an unsatisfactory performance finding has been validated, or commenced corrective action and thereafter proceeded diligently to complete such correction then the OAG may terminate this Agreement (in accordance with the "Termination of Agreement" section below) without payment to County for any costs incurred by County from the time that OAG may have commenced withholding payments due to County being in an unsatisfactory status. Where payments have been withheld and are to resume, due to County having attained satisfactory performance status, the first payment after resumption shall include all costs accrued during the period when payments to the County were withheld.

9. **AUDIT PROVISIONS**

9.1. All records, books, documents, accounting procedures, practices or any other items relevant to the performance of this Agreement shall be subject to examination or audit, and copying in

accordance with all applicable state and federal laws, rules, regulations or directives, by the OAG, the State Auditor, the U.S. Department of Health and Human Services, the Comptroller General of the United States, or any of their duly authorized representatives. The County will direct that any subcontractor with whom it has established a contractual relationship to discharge the County's obligations to likewise permit OAG, the State Auditor, the U.S. Department of Health and Human Services, and The Comptroller General of the United States, to have rights of access to, inspection of, and reproduction of all books and records of the County's subcontractor(s) which pertain to this Agreement.

- 9.2. The County shall maintain and retain for a period of three (3) years after the termination of this Agreement, or until full and final resolution of all audit or litigation matters which arise before the expiration of the three (3) year period, whichever time period is longer, such records as are necessary to fully disclose the extent of services provided under this Agreement, including but not limited to any daily activity reports and time distribution and attendance records, and other records which may show the basis of the allowable cost charges made.
- 9.3. The fiscal officer duly appointed by County shall submit a Certification of Local Expenditures Report that certifies local ICSS expenditures made by the County for contract services for the October 1 through September 31 of the fiscal year. This figure includes direct services in support of the program, allocated costs, and the costs of indirect services provided by County in support of the contracted program. This Certification is due no later than six months following the fiscal year end of the County for which the expenditures are certified. Attachment Three is included as an example form.

County shall submit two (2) copies of the Certification of Local Expenditures Report to:

Office of the Attorney General – Child Support Division  
Government Contracts Section  
PO Box 12017  
Mail Code 062  
Austin, TX 78711-2017

- 9.4. If funds are disallowed as a result of an audit finding contained in an audit (by the OAG, the State auditor, the US Department of Health and Human Services, the Comptroller General of the United States, or any of their duly authorized representatives) that the County has failed to follow federal requirements for the IV-D program, then the County agrees that the OAG may recoup their loss from funds payable under this Agreement to the extent of the loss incurred by the OAG

## 10. **TERMINATION OF AGREEMENT**

- 10.1. Discretionary Termination. The parties to this Agreement shall have the right, in each party's sole discretion and at its sole option, to terminate this Agreement by notifying the other party hereto in writing of such termination at least ninety (90) calendar days prior to the effective date of such termination. Such notice of termination shall comply with the notice provisions of the Notices Section below and shall state the effective date of such termination. Additionally a copy of any such notice by the County shall be sent by registered or certified

mail with return receipt requested, addressed to:

Office of the Texas Attorney General  
Joseph Fiore (or his successor), Mail Code 044  
Managing Attorney, Contracts Attorneys, Legal Counsel Division  
5500 E. Oltorf  
Austin, Texas 78741

- 10.2. Termination of Local Rule. The County agrees that the County local rule which deems that the part(y)(ies) to a Child support order (has) (have) made an application for Title IV-D Child Support services shall continue in effect until the termination of this Agreement (by whatever method such termination occurs).
- 10.3. Termination of Federal Waiver. The OAG agrees that termination of the Federal waiver which deems that the part(y)(ies) to a Child support order (has) (have) made an application for Title IV-D Child Support services shall not, by itself, constitute ground for termination of this agreement.
- 10.4. Post-Termination Responsibilities. Both OAG and the County agree that, upon any termination of this Agreement, a smooth transfer of pending cases and of all related child support funds is in the best interest of the public being served. OAG and County therefore agree to cooperate throughout the post-termination period and to implement a reasonable transition plan (Attachment Fourteen, a copy of which is attached hereto and included herein) designed to achieve an efficient transfer of cases, funds, and related information in a timely manner. County agrees that, if requested by OAG, County will continue to provide services under this Agreement for an additional thirty (30) calendar days beyond the termination effective date. In such event the original termination effective date shall be extended pursuant to this provision.
- 10.5. Non-exclusive Remedy. Exercise by either party of its right of early termination does not relieve either party of its obligations under this Agreement prior to its termination.

## 11. INTELLECTUAL PROPERTY OWNERSHIP

- 11.1. All work performed pursuant to the "OAG Responsibilities" section and its subsections above, which is funded by the OAG specifically including all software developed or prepared for use by the County under the terms of this Agreement, and during the term of this Agreement, is the exclusive property of the OAG. All right, title and interest in and to said property shall vest in the OAG upon creation. OAG grants to County a non-transferable and non-exclusive limited right to use the aforesaid property. County agrees that it will not otherwise copy or in any way duplicate the property, in whole or in part, except as expressly authorized to do so by prior written consent of the OAG. County shall not transfer or disclose the property to any other person or entity except for those employees of County who require such knowledge of the property in the ordinary course and scope of their employment by County. To the extent that title to any such works may not, by operation of law, vest in the OAG, all right, title and interest in such works are hereby irrevocably assigned to the OAG. The OAG shall have the right to obtain and to hold in its own name any and all patents, copyrights, registrations, or other such protection as may be appropriate to the subject matter,

and any extensions and renewals thereof. The County agrees to give the OAG as well as any person designated by the OAG all assistance reasonably required to perfect the rights, title, and interest established by this "Intellectual Property Ownership" section, without any charge or expense beyond those amounts payable to the County pursuant to the "Reimbursement of Certain Allowable Costs" and the "Federal Incentive Payments" sections and their subsections above.

**12. MAXIMUM LIABILITY OF THE OAG**

Under this Agreement, OAG liability for reimbursable expenses is limited to the amount for allowable IV-D costs incurred by the County subject to the federal financial participation rate.

Notwithstanding any other provision of this Agreement, the maximum liability of the OAG for reimbursable expenses under the terms of this Agreement is Six Hundred Eight-Five Thousand Forty-Two and no/100 Dollars (\$685,042.00).

**13. NOTICES**

13.1. Written Notice; Delivery. Any notice required or permitted to be given under this Agreement by one party to the other party shall be in writing and shall be addressed to the receiving party at the address hereinafter specified (except as provided in the "Discretionary Termination" section above). The notice shall be deemed to have been given immediately if delivered in person to the recipient's address hereinafter specified. It shall be deemed to have been given on the date of certified receipt if placed in the United States Mail, postage prepaid, by registered or certified mail with return receipt requested, addressed to the receiving party at the address hereinafter specified.

13.2. County Address. The address for the County for all purposes under this Agreement and for all notices hereunder shall be:

The Honorable Sam Biscoe (or his successor in office)  
County Judge of Travis County  
PO Box 1748  
Austin, TX 78767

with copies to (registered or certified mail with return receipt is not required for copies):

Scot Doyal, Executive Director (or his successor in office)  
Travis County Domestic Relations Office  
PO Box 1495  
Austin, TX 78767

13.3. OAG Address. The address for the OAG for all purposes under this Agreement and for all notices hereunder (except as provided in the "Discretionary Termination" section above) shall be:

Alicia Key (or her successor in office)  
Deputy Attorney General for Child Support

Office of the Attorney General  
P.O. Box 12017  
Austin, TX 78711-2017

with copies to (registered or certified mail with return receipt is not required for copies):

Joseph Fiore (or his successor in office)  
Managing Attorney, Contracts Attorneys, Legal Counsel Division  
Office of the Attorney General  
P.O. box 12017  
Austin, TX 78711-2017

- 13.4. Change of Notice Address. Each party may change the address for notice to it by giving notice of the address change as provided in this section. Notices of change of address shall be effective on the tenth (10<sup>th</sup>) calendar day following receipt of such notice.

#### **14. CONTROLLED CORRESPONDENCE**

In order to track and document requests for decisions and/or information pertaining to this Contract, and subsequent response to those requests, the OAG and the County shall use Controlled Correspondence. The OAG shall manage the Controlled Correspondence for this Contract. For each Controlled Correspondence document, the OAG shall assign a tracking number and the document shall be signed by the appropriate party's Contract Manager.

Controlled Correspondence shall not be used to change pricing or alter the terms of this Contract. Controlled Correspondence shall not be the basis of a claim for equitable adjustment of pricing. Any changes that involve the pricing or the terms of this Contract must be by a Contract amendment. However, the Controlled Correspondence process may be used to document refinements and interpretations of the provisions of this Contract and to document the cost impacts of proposed changes.

Controlled Correspondence documents shall be maintained by both Parties. Any communication not generated in accordance with such process shall not be binding upon the Parties and shall be of no effect.

#### **15. CONTRACT MANAGERS AND LIAISON PERSONNEL**

##### **15.1. The OAG Contract Manager**

Karla McDougal (or her successor in office)  
CSD-Government Contracts  
Office of the Attorney General  
PO Box 12017, Mail Code 062  
Austin, TX 78711  
[Karla.McDougal@texasattorneygeneral.gov](mailto:Karla.McDougal@texasattorneygeneral.gov)

## 15.2. The County Contract Manager

Scot Doyal  
Travis County Executive Director  
Travis County Domestic Relations Office  
PO Box 1495  
Austin, TX 78767  
[Scot.Doyal@co.travis.tx.us](mailto:Scot.Doyal@co.travis.tx.us)

### The OAG Property Liaison

Dawn Moss (or her successor in office)  
CSD-Government Contracts  
Office of the Attorney General  
PO Box 12017, Mail Code 062  
Austin, TX 78711  
[Dawn.Moss@texasattorneygeneral.gov](mailto:Dawn.Moss@texasattorneygeneral.gov)

### The County Property Liaison

Ellie Ortiz (or her successor in office)  
Travis Domestic Relations Office  
PO Box 1495  
Austin, TX 78767  
[ellie.ortiz@co.travis.tx.us](mailto:ellie.ortiz@co.travis.tx.us)

The County and the OAG shall designate Contract Managers and liaison personnel for this Agreement. The designated liaisons shall serve as the initial point of contact for any inquiries made concerning property management. The Contract Managers shall be the initial point of contact for all other matters. The Contract Managers and liaisons at the commencement of this Agreement are named. Subsequent changes in Contract Managers or liaison personnel shall be communicated by the respective parties by Controlled Correspondence.

## 16. GENERAL REQUIREMENTS

- 16.1. Procedures for Handling of Money. The County shall institute or continue to require, throughout the term of this Agreement, fiscal procedures which separate the cash handling and accounting functions. These procedures shall, at a minimum, comply with the requirements of 45 C.F.R. §302.20 and with other federal and state requirements for cash handling and accounting.
- 16.2. Use of IV-D Resources. All materials, property, personnel or services provided by the OAG shall be used by the County exclusively in the performance of this Agreement in the IV-D program.
- 16.3. Supervision of Staff. County staff and other County-provided personnel, including but not limited to private contractors retained by the County, are under the direction and supervision

of the County. The purpose of contacts between OAG employees and the County IV-D staff is communication, technical assistance and overall contract monitoring, and not for the purpose of supervision of the work of County personnel.

- 16.4. Budgetary Limitations. County will cooperatively provide the agreed to services for the Qualifying CSE Caseload. Notwithstanding any other term or condition of this Agreement, these services are subject to annual appropriation of funding by Commissioners Court into the Travis County Domestic Relations Office budget to effectively administer and enforce the agreed upon caseload. In the event such appropriation is not made, County's obligations (except for its obligation to implement, in conjunction with the OAG, the transition plan developed in accordance with the Post-Termination Responsibilities section above) under this Agreement shall end simultaneous with the termination of such appropriation. County shall notify OAG in writing of its decision to terminate funding within ten (10) days of the date that the decision to terminate funding is made. OAG (concomitantly with the cessation of County's obligations under this Agreement) shall have no further obligations under this Agreement except for its obligation to implement, in conjunction with the County, the transition plan developed in accordance with the Post-Termination Responsibilities section above.

All obligations of the OAG are subject to the availability of legislative appropriations and, to the availability of federal funds applicable to this Agreement. The parties acknowledge that the ability of the OAG to make payments under this contract is contingent upon the continued availability of funds for the Child Support Enforcement Strategy and the State Disbursement Unit Strategy (collectively "Strategies"). The parties acknowledge that funds are not specifically appropriated for this contract and the OAG's continual ability to make payments under this contract is contingent upon the funding levels appropriated to the OAG for the Strategies for each particular appropriation period. The OAG will use all reasonable efforts to ensure that such funds are available. The parties agree that if future levels of funding for the OAG Child Support Enforcement Strategy and/or the State Disbursement Unit Strategy and/or federal funds are not sufficient to continue operations without any operational reductions, the OAG, in its discretion, may terminate this contract, either in whole or in part. In the event of such termination, the OAG's obligations (except for its obligation to implement, in conjunction with the County, the transition plan developed in accordance with the Post-Termination Responsibilities section above) under this Agreement shall end simultaneous with the termination of either appropriated funds or federal funds and OAG shall notify County within ten (10) days of such fact in writing. County (concomitantly with the cessation of OAG's obligations under this Agreement) shall have no further obligations under this Agreement except for its obligation to implement, in conjunction with the OAG, the transition plan developed in accordance with the Post-Termination Responsibilities section above.

- 16.5. Property Management, Accountability and Maintenance.

- 16.5.1. All equipment provided by the OAG under this Agreement (including but not limited to personal computers, hardware, peripheral devices, and software) shall remain the property of the OAG and all titles and rights remain with the OAG. Prior to installation of OAG equipment, County shall verify the asset information listed on the OAG Interdepartmental Equipment Transfer (IDET) form (Attachment Four; incorporated

herein and made a part hereof), provide the OAG with the physical address and actual location of each piece of OAG provided equipment, and acknowledge County's receipt, as well as, fiduciary and pecuniary responsibility with its signature. Forms shall be returned, with original signature, to OAG Property Liaison. OAG shall provide through the OAG Property Liaison on a monthly basis a listing of all OAG inventoried equipment provided to County. County shall verify these monthly inventory reports and return them to the OAG Property Liaison. County shall designate a custodian for the equipment and respond to all OAG inventory and custodian verification requests within five (5) working days of receipt of the request. In the event that the physical address or actual location of any piece of equipment changes, County agrees to provide the new physical address or new actual location to the OAG within five (5) working days.

- 16.5.2. County shall maintain a control system to insure adequate safeguards to prevent loss, damage, or theft of the equipment. In the case of equipment with an OAG inventory tag, County shall have each person provided with such equipment complete an Acknowledgment of Custodianship of Office of the Attorney General Equipment form (Attachment Five; incorporated herein and made a part hereof). Forms shall be returned to OAG Property Liaison. County shall report any loss, damage or theft of the equipment to OAG within one (1) workday of discovery of same. County shall be liable for any loss, damage or theft of the equipment due to the negligent or intentional wrongful acts of or the failure to exercise reasonable care for the equipment's safekeeping on the part of County, its agents or its contractors. In the event of missing property, the County Property Liaison shall make every attempt to locate the item. If the missing item is not found within one (1) work day a Lost or Stolen Property Report (Attachment Six; incorporated herein and made a part hereof) shall be submitted to the OAG Property Liaison. If there is a suspicion of theft, County shall notify the local police department immediately and a copy of the police incident report shall also be submitted to the OAG Property Liaison.
- 16.5.3. Equipment provided to County by OAG under this Agreement may only be used for IV-D functions.
- 16.5.4. County shall comply with all license agreements associated with OAG-provided software and shall not install any software upgrades or programs on any hardware provided by OAG.
- 16.5.5. OAG shall have all reasonable rights of access to the equipment provided by OAG during County's normal business hours.
- 16.5.6. County shall assist OAG in complying with the federal uniform standards governing management and disposition of property furnished by or whose cost was charged directly to a project supported by funding administered by the U.S. Department of Health and Human Services as well as all applicable state requirements governing the procurement, management, and disposition of property. Such requirements include marking such property, maintenance of detailed inventory records, and completion of a physical inventory. Property subject to this requirement includes any and all fixed assets or other property procured with the aid of federal funds. All disposition of OAG provided equipment will be performed by OAG.



- 16.5.7. County shall maintain and administer in accordance with good business practices a program for the protection and preservation of property provided to County in the performance of this Agreement. Repairs and maintenance of the OAG provided equipment shall be the responsibility of OAG.
- 16.6. Modification. This Agreement may be modified by mutual agreement of the parties at anytime, provided that said modification shall be made in a written addendum to this Agreement signed by both parties.
- 16.7. Confidentiality and Security Provisions.
- 16.7.1. General.
- 16.7.1.1. Both OAG and County recognize and assume the duty to protect and safeguard confidential information. Confidential information specifically includes personally identifiable information such as Social Security Number, full name, date of birth, home address, account number, and case status. Each entity acknowledges that the loss of confidentiality, integrity and availability of information assets is a risk which can be minimized by effective security safeguards and enforced compliance with information security policies, standards and procedures.
- 16.7.1.2. OAG recognizes that County has existing statutory responsibilities to maintain confidentiality of records related to state district courts (juvenile, family, probate, civil and criminal), county courts and national and state criminal records (FBI, NCIC, TCIC). OAG also recognizes that County has existing processes and procedures that ensure the security and confidentiality of this information and data and is subject to security audits or assessments by these authorities.
- 16.7.1.3. This agreement requires County to retrieve data from the courts and other sources and create data within TXCSES.
- 16.7.1.4. County acknowledges and agrees to protect OAG Data as confidential. All references to "OAG Data" shall mean all data and information (i) originated by OAG and/or submitted to County by or on behalf of OAG, or (ii) which County accesses from OAG systems in connection with provision of the Agreement Services. OAG Data does not include data and information originated by County in the performance of its duties. Upon request by OAG, County shall execute and deliver any documents that may be necessary or desirable under any law to preserve or enable OAG to enforce its rights with respect to OAG Data. Tex. Gov't Code Chapter 552 defines the exclusive mechanism for determining whether OAG Data are subject to public disclosure. However, data that is publicly known and generally available to the public is not subject to these Confidentiality and Security Provisions.
- 16.7.1.5. If any term or provision of this Confidentiality and Security Provision, shall be found to be illegal or unenforceable, it shall be deemed independent and divisible,

and notwithstanding such illegality or unenforceability, all other terms or provisions in this Confidentiality and Security Provision, shall remain in full force and effect and such illegal or unenforceable term or provision shall be deemed to be deleted.

- 16.7.1.6. County shall develop and implement access protection lists. The access protection lists shall document the name and other identifying data for any individual, authorized pursuant to County's request, to access, use or disclose OAG Data, as well as any special conditions and limitations applicable to each authorization. County shall remove individuals from or change the access rights of individuals on the access protection list immediately upon such individual no longer requiring access. At least monthly, OAG shall send County a list of TXCSES users and County shall review and update its access protection lists and ensure that the access protection lists accurately reflect the individuals and their access level currently authorized. County shall notify OAG of the authorized personnel that should have access rights to OAG Data and information in the method prescribed by OAG. County will immediately notify OAG when an individual's access to OAG systems is no longer relevant. OAG, in its sole discretion, may deny or revoke an individual's access to OAG Data and information and any of its systems.
- 16.7.1.7. County shall perform background reviews, to include a criminal history record review, on all County employees who will have access to OAG Data and information, and any OAG system. County shall certify to OAG that such reviews have been conducted and that in County's opinion the aforesaid employees are deemed trustworthy. County may request OAG to perform such reviews. In such instances, County shall provide OAG with any required information, consent and authorization to perform the reviews and OAG shall perform the reviews at its own expense.
- 16.7.1.8. All references to "Agreement Services" shall include activities within the scope of this Agreement.
- 16.7.1.9. County shall comply with all applicable statutory and regulatory provisions requiring that information be safeguarded and kept confidential. These statutes and regulatory provisions include but are not limited to 42 U.S.C. §§ 653 and 654; 45 CFR §§ 307.10, 307.11 and 307.13; 26 U.S.C. 6103 (IRC 6103); IRS Publication 1075 (Rev. 8-2010) and § 231.108 of the Texas Family Code, each as currently written or as may be amended, revised or enacted. County shall also comply with OAG policy, processes and procedures concerning the safeguarding and confidentiality of information, and computer security (including the posting of Attachment Thirteen, "IRS Notice", in all County work areas affected by this Agreement and any requirements set forth in Attachment Seven, entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information"). The requirements of these Confidentiality and Security Provisions shall be included in, and apply to, subcontracts and agreements County has with anyone performing Agreement Services on County's behalf.

16.7.1.10. This Agreement is between County and OAG, and is not intended to create any independent cause of action by any third party, individual, or entity against OAG or County.

**16.7.2. OAG Data Usage and Storage.**

- 16.7.2.1. County agrees to maintain physical security for OAG data by maintaining an environment designed to prevent loss or unauthorized removal of data. County shall ensure that all persons having access to data obtained from OAG Systems are thoroughly briefed on related security procedures, use restrictions, and instructions requiring their awareness and compliance. County shall ensure that all County personnel having access to OAG Data receive annual reorientation sessions when offered by the OAG and all County personnel that perform or are assigned to perform Agreement Services shall re-execute, and/or renew their acceptance of, all applicable security documents and to ensure that they remain alert to all security requirements. County personnel shall only be granted access to OAG Systems after they have received all required security training, read the OAG Data Security Policy Manual (Attachment Eight), signed the acknowledgment (and County has given the signed acknowledgment to the OAG Contract Manager) and read and accepted the OAG Automated Computer System Access Statement of Responsibility (Attachment Nine), and read and signed the IRS Information Notification Form (Attachment Ten).
- 16.7.2.2. OAG Data are not allowed on mobile/remote/portable storage devices; nor may storage media be removed from the facility used by County. Any exception to this prohibition must have OAG prior approval. Such approval may only be granted by Controlled Correspondence or Contract amendment. This prohibition does not apply to County Information Systems backup procedure. County Information Systems backup procedure is subject to the United States Internal Revenue Service requirements set forth in IRS Publication 1075 (Rev.8/2010) and Attachment Seven entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information".
- 16.7.2.3. County stipulates, covenants, and agrees that it will not access, use or disclose OAG Data beyond its limited authorization, or for any purpose not necessary for the performance of its duties under this Agreement. Without OAG's approval (in its sole discretion), County will not: (i) use OAG Data other than in connection with providing the Agreement Services; (ii) disclose, sell, assign, lease, or otherwise provide OAG Data to third parties, including any local, state, or Federal legislative body; (iii) commercially exploit OAG Data or allow OAG Data to be commercially exploited; or (iv) create, distribute or use any electronic or hard copy mailing list of OAG Customers for purposes other than in connection with providing the Agreement Services. However, nothing in this agreement is intended to restrict County from performing its other authorized duties. For example, the duty to disseminate copies of court orders to requesting parties that necessarily includes data such as names and addresses. In the event that County

fails to comply with this subsection, OAG may exercise any remedy, including immediate termination of this Agreement.

- 16.7.2.4. County agrees that it shall comply with all state and federal standards regarding the protection and confidentiality of OAG Data as currently effective, subsequently enacted or as may be amended. OAG Data accessed shall always be maintained in a secure environment (with limited access by authorized personnel both during work and non-work hours) using devices and methods such as, but not limited to: alarm systems, locked containers of various types, fireproof safes, restricted areas, locked rooms, locked buildings, identification systems, guards, or other devices reasonably expected to prevent loss or unauthorized removal of manually held data. County shall also protect against unauthorized use of passwords, keys, combinations, access logs, and badges. Whenever possible, computer operations must be in a secure area with restricted access. In situations such as remote terminals, or office work sites where all of the requirements of a secure area with restricted access cannot be maintained, the equipment shall receive the highest level of protection.

**16.7.3. OAG Data Retention and Destruction, and Public Information Requests.**

- 16.7.3.1. Within ninety (90) calendar days of this Agreement's execution, County and OAG shall develop a detailed schedule for the retention and possible destruction of OAG Data. The schedule will be based upon the Agreement Services being performed and the County's limited authorization to access, use, and disclose OAG Data.
- 16.7.3.2. Any destruction or purging of OAG Data shall be destroyed and/or purged in accordance with state and federal statutes, rules and regulations. Within ten (10) business days of destruction or purging, County will provide the OAG with a signed statement(s) containing the date of destruction or purging, description of OAG Data destroyed or purged, and the method(s) used.
- 16.7.3.3. In the event of Agreement expiration or termination for any reason, County shall ensure the security of any OAG Data remaining in any storage component to prevent unauthorized disclosures. Within twenty (20) business days of Agreement expiration or termination, County shall provide OAG with a signed statement detailing the nature of the OAG Data retained, type of storage media, physical location(s), and any planned destruction date.
- 16.7.3.4. County expressly does not have any actual or implied authority to determine whether any OAG Data are public or exempted from disclosure. County is not authorized to respond to public information requests which would require disclosure of otherwise confidential information on behalf of the OAG. County agrees to forward to the OAG, by facsimile within one (1) business day from receipt all request(s) for information associated with the County's services under this Agreement. County shall forward any information requests to:

Public Information Coordinator

**16.7.4. Security Incidents.**

**16.7.4.1. Response to Security Incidents.**

**16.7.4.1.1. County shall respond to detected security incidents. The term “security incident” means an occurrence or event where the confidentiality of OAG Data may have been compromised. County shall maintain an internal incident response plan to facilitate a quick, effective and orderly response to information security incidents. The incident response plan should cover such topics as:**

- 1. Initial responders**
- 2. Containment**
- 3. Management Notification**
- 4. Documentation of Response Actions**
- 5. Expedious confirmation of system integrity**
- 6. Collection of audit trails and similar evidence**
- 7. Cause analysis**
- 8. Damage analysis and mitigation**
- 9. Internal Reporting Responsibility**
- 10. External Reporting Responsibility**
- 11. OAG Contract Manager’s and OAG CISO’s name, phone number and email address**

**Attachment Eleven is County’s current internal incident response plan. Any changes to this incident response plan require OAG approval (which approval shall not be unreasonably withheld) and may be made by Controlled Correspondence**

**16.7.4.2. Notice.**

**16.7.4.2.1. Within one (1) hour of concluding that there has been, any OAG Data security incident County shall initiate damage mitigation and notify the OAG Chief Information Security Officer (“OAG CISO”) and the OAG Contract Manager, by telephone and by email, of the security incident and the initial damage mitigation steps taken. Current contact information shall be contained in the Incident Response Plan.**

**16.7.4.2.2. Within twenty-four (24) hours of the discovery, County shall conduct a preliminary damage analysis of the security incident; commence an investigation into the incident; and provide a written report to the OAG CISO, with a copy to the OAG Contract Manager fully disclosing all information relating to the security incident and the results of the preliminary damage analysis. This initial report shall include, at a minimum: time and nature of the incident (e.g., OAG data loss/corruption/intrusion); cause(s); mitigation**

efforts; corrective actions; and estimated recovery time.

16.7.4.2.3. Each day thereafter until the investigation is complete, County shall: (i) provide the OAG CISO, or the OAG CISO's designee, with a daily oral or email report regarding the investigation status and current damage analysis; and (ii) confer with the OAG CISO, or the OAG CISO's designee, regarding the proper course of the investigation and damage mitigation.

16.7.4.2.4. Whenever daily oral reports are provided, County shall provide, by close of business each Friday, an email report detailing the foregoing daily requirements.

16.7.4.3.

Final Report.

16.7.4.3.1. Within five (5) business days of completing the damage analysis and investigation, County shall submit a written Final Report to the OAG CISO with a copy to the OAG Contract Manager, which shall include:

16.7.4.3.1.1. A detailed explanation of the cause(s) of the security incident;

16.7.4.3.1.2. A detailed description of the nature of the security incident, including, but not limited to, extent of intruder activity (such as files changed, edited or removed; Trojans), and the particular OAG Data affected; and

16.7.4.3.1.3. A specific cure for the security incident and the date by which such cure shall be implemented, or if the cure has been put in place, a certification to OAG that states the date County implemented the cure, a description of how the cure protects against the possibility of a recurrence, and that County's security program is operating with the effectiveness required to assure that the security, confidentiality and integrity of OAG Data are protected.

16.7.4.3.2. If the cure has not been put in place by the time the report is submitted, County shall within five (5) business days after submission of the final report, provide a certification to OAG that states the date County implemented the cure, a description of how the cure protects against the possibility of a recurrence, and that County's security program is operating with the effectiveness required to assure that the security, confidentiality and integrity of OAG Data are protected.

16.7.4.3.3. If County fails to provide a Final Report or Certification within fifteen (15) calendar days of the security incident, County agrees that OAG may exercise any right, remedy or privilege which may be available to it under applicable law of the State and any other applicable law. The exercise of any of the foregoing remedies will not constitute a termination of this Agreement unless OAG notifies County in writing prior to the exercise of such remedy.

16.7.4.4. Independent Right to Investigate.

16.7.4.4.1. OAG reserves the right to conduct an independent investigation of any security incident, and should OAG choose to do so, County shall cooperate fully, making resources, personnel and systems access available. If at all possible, OAG will provide reasonable notice to County that it is going to conduct an independent investigation.

16.7.4.5.

Security Audit.

16.7.4.5.1. Right to Audit, Investigate and Inspect the Facilities, Operations, and Systems Used in the Performance of Agreement Services.

16.7.4.5.1.1. County shall permit OAG, the State Auditor of Texas, the United States Internal Revenue Service, the United States Department of Health and Human Services and the Comptroller General of the United States to:

16.7.4.5.1.2. monitor and observe the operations of, and to perform security investigations, audits and reviews of the operations and records of, the County;

16.7.4.5.1.3. inspect its information system in order to access security at the operating system, network, and application levels; provided, however, that such access shall not interfere with the daily operations of managing and running the system;

16.7.4.5.1.4. enter into the offices and places of business of County and County's subcontractors for a security inspection of the facilities and operations used in the performance of Agreement Services. Specific remedial measures may be required in cases where County or County's subcontractors are found to be noncompliant with physical and/or OAG data security protection.

16.7.4.5.1.5. When OAG performs any of the above monitoring, observations, and inspections, OAG will provide County with reasonable notice that conforms to standard business audit protocol. However prior notice is not always possible when such functions are performed by the State Auditor of Texas, the United States Internal Revenue Service, the United States Department of Health and Human Services and the Comptroller General of the United States. In those instances the OAG will endeavor to provide as much notice as possible but the right to enter without notice is specifically reserved.

16.7.4.5.1.6. Any audit of documents shall be conducted at County's principal place of business and/or the location(s) of County's operations during County's normal business hours and at OAG's expense. County shall provide on County's premises, (or if the audit is being performed of a County's subcontractor, the County's subcontractor's premises, if

necessary) the physical and technical support reasonably necessary for OAG auditors and inspectors to perform their work.

16.7.5.

Remedial Action.

16.7.5.1. Remedies Not Exclusive and Injunctive Relief.

16.7.5.1.1. The remedies provided in this section are in addition to, and not exclusive of, all other remedies available within this Agreement, or at law or in equity. OAG's pursuit or non-pursuit of any one remedy for a security incident(s) does not constitute a waiver of any other remedy that OAG may have at law or equity.

16.7.5.1.2. If injunctive or other equitable relief is available, then County agrees that OAG shall not be required to post bond or other security as a condition of such relief.

16.7.5.2. Notice to Third Parties.

16.7.5.2.1. Subject to OAG review and approval, County shall provide notice to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the security incident, with such notice to include: (i) a brief description of what happened; (ii) to the extent possible, a description of the types of personal data that were involved in the security breach (e.g., full name, SSN, date of birth, home address, account number, etc.); (iii) a brief description of what is being done to investigate the breach, mitigate losses, and to protect against any further breaches; (iv) contact procedures for those wishing to ask questions or learn additional data, including a telephone number, website, if available, and postal address; and, (v) instructions for accessing the Consumer Protection Identity Theft section of the OAG website. County and OAG shall mutually agree on the methodology for providing the notice.

16.7.5.2.2. County shall be responsible for responding to and following up on inquiries and requests for further assistance from persons notified under the preceding section.

16.7.5.2.3. If County does not provide the required notice, OAG may elect to provide notice of the security incident. County and OAG shall mutually agree on the methodology for providing the notice. Costs (excluding personnel costs) associated with providing notice shall be reimbursed to OAG by County. If County does not reimburse such cost within thirty (30) calendar days of request, OAG shall have the right to collect such cost. Additionally, OAG may collect such cost by offsetting or reducing any future payments owed to County.



- 16.7.6. Commencement of Legal Action.
- 16.7.6.1. County shall not commence any legal proceeding on OAG's behalf outside the scope of the Agreement Services without OAG's express written consent. OAG shall not commence any legal proceedings on County's behalf without County's express written consent.
- 16.7.7. Survival of Provisions.
- 16.7.7.1. Perpetual Survival and Severability.
- 16.7.7.1.1. OAG rights and privileges applicable to OAG Data, including the confidentiality and security thereof, shall survive expiration or any termination of this Agreement, and shall be perpetual.
- 16.8. Political Activities. As required by 5 U.S.C. § 1501 *et seq.*, none of the resources contributed by the OAG or the County pursuant to this Agreement shall be used in the performance of any partisan political activity or to further the election or defeat of any candidate for public office.
- 16.9. Acknowledgment of Funding. The County agrees to place in any literature describing the services covered under this Agreement (as well as in all reports of investigations, studies, and other materials) notices acknowledging the funding provided by the OAG and the federal Office of Child Support Enforcement to the County. Such notices also shall be placed in the County's annual reports. All such literature, reports, and other materials shall be the joint property of the parties to this Agreement.
- 16.10. Assignment. Neither this Agreement nor any rights, services, duties or responsibilities hereunder shall be assigned or delegated by either party in whole or in part without the prior written consent of the other party.
- 16.11. Subcontracting. The County shall not subcontract any portion of the IV-D services to be performed under this Agreement without the prior written approval of the OAG. All subcontracts, if any, entered into by the County shall be written and competitively advertised. Any subcontract entered into by the County shall be subject to the requirements of this Agreement. The County agrees to be responsible to the OAG for the performance of any subcontractor and remains bound to perform the duties described in any subcontract regardless of whether the subcontractor breaches in its performance. The County understands and acknowledges that the OAG is in no manner liable to any subcontractor of the County.
- 16.12. Compliance with Other Requirements. The County shall comply with all federal and state laws, rules, regulations, requirements and guidelines applicable to County: (1) performing its obligations hereunder and to assure, with respect to its performances hereunder, that the OAG is fully and completely meeting obligations imposed by all laws, rules, regulations, requirements, and guidelines upon the OAG in carrying out the ICSS program pursuant to Chapter 231 of the Texas Family Code and Title IV, Part D, of the Social Security Act of 1935, as amended; (2) providing services to OAG as these laws,

rules, regulations, requirements and guidelines currently exist and as they are amended throughout the term of this Agreement. Notwithstanding anything to the contrary in this Agreement, OAG reserves the right, in its sole discretion, to unilaterally amend this Agreement throughout its term to incorporate any modifications necessary for OAG's or County's compliance with all applicable state and federal laws, rules, regulations, requirements and guidelines.

16.13. Computer Generated Data Disclaimer.

**THE OAG MAKES NO REPRESENTATION AND NO WARRANTIES, EITHER EXPRESS OR IMPLIED, AS TO THE ACCURACY OF COMPUTER GENERATED DATA, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES, IF ANY, OF MERCHANTABILITY AND FITNESS FOR ANY PARTICULAR PURPOSE.**

**COUNTY MAKES NO REPRESENTATION AND NO WARRANTIES, EITHER EXPRESS OR IMPLIED, AS TO THE ACCURACY OF COMPUTER GENERATED DATA, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES, IF ANY, OF MERCHANTABILITY AND FITNESS FOR ANY PARTICULAR PURPOSE.**

**NEITHER PARTY SHALL BE LIABLE FOR ANY LOST PROFITS, LOST SAVINGS OR OTHER CONSEQUENTIAL DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF OR COULD HAVE FORESEEN SUCH DAMAGES. BOTH PARTIES AGREE THAT THE SOLE AND EXCLUSIVE REMEDIES FOR ANY COMPUTER INFORMATION PROBLEM SHALL BE EITHER (1) THE CORRECTION OF THE SOURCE OF THE COMPUTER RELATED PROBLEM, BY THE PARTY WITH CONTROL OF THE SOURCE OR THE ERROR, OR (2) TERMINATION OF THIS AGREEMENT.**

16.14. Independent Contractor. It is expressly understood and agreed by the parties hereto that the County is an independent contractor. It is further expressly understood and agreed that any County personnel employed or retained to carry out the terms of this Agreement are deemed to be the employees and/or agents of the County for the purposes of retirement benefits, health insurance, all types of leave, and for any and all other purposes.

16.15. Civil Rights. County agrees that no person shall, on the ground of race, color, religion, sex, national origin, age, disability, political affiliation, or religious belief, be excluded from the participation in, be denied the benefits of, be subjected to discrimination under, or be denied employment in the administration of, or in connection with, any program or activity funded in whole or in part with funds available under this Agreement. County shall comply with Executive Order 11246, "Equal Employment Opportunity" as amended by Executive Order 11375, "Amending Executive Order 11246 relating to Equal Employment Opportunity", and as supplemented by regulations at 41 C.F.R. Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity

Department of Labor". County shall ensure that all subcontracts comply with the above referenced provisions.

- 16.16. **Environmental Protection.** County shall be in compliance with all applicable standards, orders, or requirements issued pursuant to the mandates of the Clean Air Act (42 U.S.C. Section 7401 *et seq.*) and the Federal Water Pollution Control Act, as amended, (33 U.S.C. 1251 *et seq.*).
- 16.17. **Certain Disclosures Concerning Lobbying.** County shall comply with the provisions of a federal law known generally as the Lobbying Disclosure Acts of 1989, and the regulations of the United States Department of Health and Human Services promulgated pursuant to said law, and shall make all disclosures and certifications as required by law. County must sign and return the Certification Regarding Lobbying included in this Agreement as Attachment Twelve. This certification certifies that the County will not and has not used federally appropriated funds to pay any person or organization for influencing or attempting to influence any officer or employee of any Federal agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal Contract, grant or any other award covered by 31 U.S.C. 1352. It also certifies that the County will disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award by completing and submitting Standard Form LLL.
- 16.18. **Dispute Resolution Process for County Breach of Contract Claim**
  - 16.18.1. The dispute resolution process provided for in Chapter 2260 of the Government Code shall be used, as further described herein, by the OAG and County to attempt to resolve any claim for breach of contract made by County.
  - 16.18.2. A County claim for breach of this Agreement that the parties cannot resolve in the ordinary course of business shall be submitted to the negotiation process provided in Chapter 2260, subchapter B, of the Government Code. To initiate the process, the County shall submit written notice, as required by subchapter B, to the Director, Child Support Division, Office of the Attorney General, P.O. Box 12017 (Mail Code 033), Austin, Texas 78711-2017. Said notice shall specifically state that the provisions of Chapter 2260, subchapter B, are being invoked. A copy of the notice shall also be given to all other representatives of the OAG and County otherwise entitled to notice under this Agreement. Compliance by County with subchapter B is a condition precedent to the filing of a contested case proceeding under Chapter 2260, subchapter C, of the Government Code.
  - 16.18.3. The contested case process provided in Chapter 2260, subchapter C, of the Government Code is the County's sole and exclusive process for seeking a remedy for any and all alleged breaches of contract by the OAG if the parties are unable to resolve their disputes under the immediately preceding section.
  - 16.18.4. Compliance with the contested case process provided in subchapter C is a condition precedent to seeking consent to sue from the Legislature under Chapter 107 of the Civil Practices and Remedies Code. Neither the execution of this

Agreement by the OAG nor any other conduct of any representative of the OAG relating to the Agreement shall be considered a waiver of sovereign immunity to suit.

- 16.18.5. The submission, processing and resolution of the County's claim is governed by the published rules adopted by the OAG pursuant to Chapter 2260, as currently effective, hereafter enacted or subsequently amended.
- 16.18.6. Neither the occurrence of an event nor the pendency of a claim constitutes grounds for the suspension of performance by County, in whole or in part.
- 16.19. News Releases or Pronouncements. News releases and/or advertisements, publications, declarations and any other pronouncements, not required by law, pertaining to this transaction by the County, using any means or media, must be approved in writing by the OAG prior to public dissemination.
- 16.20. Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion from Participation in Contracts Exceeding \$100,000.00. County certifies by entering into this Agreement, that neither it nor its principals are debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency. The certification requirement of this provision shall be included in all subcontracts that exceed \$100,000.
- 16.21. Reporting Fraud, Waste or Abuse. The Contractor must report any suspected incident of fraud, waste or abuse associated with the performance of this Contract to any one of the following listed entities:
- the Contract Manager;
  - the Deputy Director for Contract Operations, Child Support Division;
  - the Director, Child Support Division;
  - the Deputy Director, Child Support Division;
  - the OAG Ethics Advisor;
- the OAG's Fraud, Waste and Abuse Prevention Program ("FWAPP") Hotline (866-552-7937) or the FWAPP E-Mailbox (FWAPP@oag.state.tx.us);
- the State Auditor's Office hotline for fraud (1-800-892-8348).
- The report of suspected misconduct shall include (if known):
- the specific suspected misconduct;
  - the names of the individual(s)/entity(ies) involved;
  - the date(s)/location(s) of the alleged activity(ies);
  - the names and all available contact information (phone numbers, addresses) of possible witnesses or other individuals who may have relevant information; and
  - any documents which tend to support the allegations.

- 16.21.1. The words fraud, waste or abuse as used in this Section have the following meanings:

Fraud is the use of one's position for obtaining personal benefit (including benefit for family/friends) through the deliberate misuse or misapplication of resources or assets.

Waste is the extravagant careless or needless expenditure of funds or consumption of property that results from deficient practices, system controls, or decisions.

Abuse, is the misuse of one's position, title or authority to obtain a personal benefit (including benefit for family/friends) or to attempt to damage someone else.

- 16.22. Non-Waiver of Rights. Failure of a party to require performance by another party under this Agreement will not affect the right of such party to require performance in the future. No delay, failure, or waiver of either party's exercise or partial exercise of any right or remedy under this Agreement shall operate to limit, impair, preclude, cancel, waive or otherwise affect such right or remedy. A waiver by a party of any breach of any term of this Agreement will not be construed as a waiver of any continuing or succeeding breach. Should any provision of this Agreement be invalid or unenforceable, the remainder of the provisions will remain in effect.
- 16.23. Offshoring. All work to be performed under this Agreement shall be performed within the United States and its territories.
- 16.24. Section 2261.053, Government Code, prohibits the OAG from awarding a contract to any entity which, in the past five years, has been convicted of violating a federal law or assessed a penalty in connection with a contract involving relief for Hurricane Rita, Hurricane Katrina, or any other disaster, as defined by §418.004 of the Government Code, occurring after September 24, 2005. Under §2261.053, Government Code, the County certifies that it is not ineligible to receive this Agreement and acknowledges that the Agreement may be terminated and payment withheld if this certification is inaccurate
- 16.25. Assignment of Claims. County hereby assigns to the OAG any claims for overcharges associated with this Agreement under 15 U.S.C. §1, *et seq.*, and Tex. Bus. & Comm. Code §15.01, *et seq.*
- 16.26. Certification Concerning Dealings with Public Servants. County, by signing this Agreement, certifies that it has not given nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this transaction.
- 16.27. Personnel Comportment. County and County subcontractor personnel and agents shall be courteous and professional in all communications during their performance of the requirements of this Agreement. Any actions deemed unprofessional must be remedied to the satisfaction of the OAG Contract Manager. The OAG reserves the right, in its sole discretion, to require the immediate removal and replacement of any County and/or County subcontractor personnel and agents deemed by the OAG to be discourteous, unprofessional, unsuitable or otherwise objectionable. Any replacement personnel assigned by County to perform services under this Agreement must have qualifications for the assigned position that equal or exceed those of the person being replaced
- 16.28. Applicable Law and Venue. County agrees that this Agreement in all respects shall be

governed by and construed in accordance with the laws of the State of Texas, except for its provisions regarding conflicts of laws. County also agrees that the exclusive venue and jurisdiction of any legal action or suit brought by County concerning this Agreement is, and that any such legal action or suit shall be brought, in a court of competent jurisdiction in Travis County, Texas. OAG agrees that any legal action or suit brought by OAG concerning this Agreement shall be brought in a court of competent jurisdiction in Travis County. County further agrees that all payments shall be due and payable in Travis County, Texas.

- 16.29. Headings. The headings for each section of this Agreement are stated for convenience only and are not to be construed as limiting.
- 16.30. Survival of Terms. Termination of this Agreement for any reason shall not release County from any liability or obligation set forth in this Agreement that is expressly stated to survive any such termination or by its nature would be intended to be applicable following any such termination.
- 16.31. Entire Agreement. This instrument constitutes the entire Agreement between the parties hereto, and all oral or written agreements between the parties hereto relating to the subject matter of this Agreement that were made prior to the execution of this Agreement have been reduced to writing and are contained herein.
- 16.32. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.
- 16.33. Attachments.
- 16.33.1. Attachment One is attached to this Agreement for the sole purpose of illustrating the allocation calculations which the OAG will perform in allocating any bonus allocations for incentive revenues earned by counties participating in cooperative agreements to enhance the delivery of IV-D services to Texas citizens.
  - 16.33.2. Attachment Two, "Sampling Methodology for Quality and Efficiency Standards"
  - 16.33.3. Attachment Three, "Certification of Local Expenditures Report"
  - 16.33.4. Attachment Four, "Inter-departmental Equipment Transfer" shall be verified or prepared and signed by County to acknowledge the movement of equipment and software between the County and the OAG.
  - 16.33.5. Attachment Five, "Acknowledgment of Custodianship of Office of the Attorney General Equipment" form shall be completed by each person provided with equipment with an OAG inventory tag.
  - 16.33.6. Attachment Six, "Lost or Stolen Property Report" shall be completed by County upon determination of OAG equipment being lost or stolen and forwarded to the OAG liaison.

- 16.33.7 Attachment Seven is the "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information".
- 16.33.8 Attachment Eight is the OAG Information Security Policy Manual which all County personnel obtaining access to the OAG system must read.
- 16.33.9 Attachment Nine represents the OAG Statement of Responsibility which all County personnel requesting access to the OAG system must complete and sign.
- 16.33.10 Attachment Ten, AIRS Information: Notification Form", shall be read and signed by all County Personnel requesting access to the OAG system.
- 16.33.11 Attachment Eleven is the County's "Internal Incident Response Plan" which shall be used to facilitate a quick, effective and orderly response to information security incidents.
- 16.33.12 Attachment Twelve, ACertification Regarding Lobbying@, shall be signed by the County and returned with executed Agreement.
- 13.66.13 Attachment Thirteen, AIRS Notice@, shall be posted by the County in all County work areas affected by this Agreement.
- 16.33.14 Attachment Fourteen, ATermination Transition Plan@

THIS AGREEMENT IS HEREBY ACCEPTED.

FOR THE COUNTY:

FOR THE OFFICE OF THE ATTORNEY GENERAL:

\_\_\_\_\_  
 The Honorable Sam Biscoe  
 County Judge, Travis County

\_\_\_\_\_  
 Alicia G. Key  
 Deputy Attorney General for Child Support

Date \_\_\_\_\_

Date \_\_\_\_\_

## SAMPLE Estimate County Share of Incentives

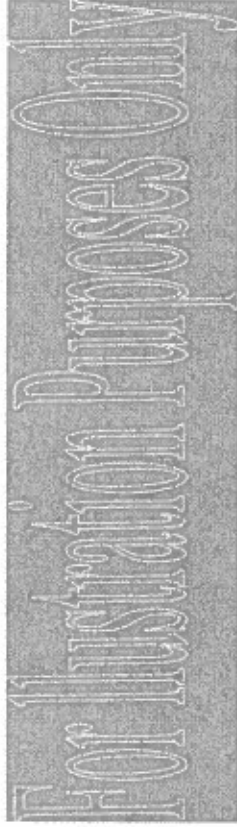
Federal Fiscal Year	[A] Measurement	[B] Estimated County Collections	[C] = [A] + [B] Texas Collections Base	[D] Cnty to Coll Base Ratio	[E] = [D] X [C] Texas Performance Incentives	[F] = [E] X [F] County Revenue Allocation	[G] = [E] X [F] Field Office Percentage	[H] = [G] X [F] Projected Incentives
	CCS	\$75,000,000	4,000,000,000	1.875%	\$8,500,000	\$159,375.00	33.20%	\$52,912.50
	COA	\$75,000,000	4,000,000,000	1.875%	\$7,000,000	\$131,250.00	33.20%	\$43,575.00
	Cost Effect	\$75,000,000	4,000,000,000	1.875%	\$9,000,000	\$168,750.00	33.20%	\$56,025.00

*estimated*

Minimum Score	Score	Applicable Percentage
CCS	63%	80.0%
COA	65%	80.0%
Cost Effect	\$7.50	\$53.72

### County Share of Federal Incentives\*:

Collections on Current Support	\$52,912.50
Collections on Arrears	\$43,575.00
<b>Cost Effectiveness</b>	<b>\$56,025.00</b>
<b>Total County Share of Incentives:</b>	<b>\$152,512.50</b>



\* County Cost Effectiveness must be equal to or greater than State cost effectiveness, based on ICSS Annual Reports and OSCE Reports  
 \* Projected Incentive X Applicable Percentage



## Sampling Methodology for Quality and Efficiency Standards

For the purposes of statistical sampling to determine Exceptional Performance, the OAG plans to evaluate the County's achievement of both the Minimum and Exceptional Quality and Efficiency (Q&E) Standards using statistical sampling and sample results evaluation as follows:

- Cases and/or case activities where any Q&E Measurement is relevant for a specific month represent a statistical population, and each sampled case or case activity is a sample item.
- The OAG will select a sample and review sample items to assess achievement of the Minimum Standard and Exceptional Standard in a manner that can be statistically generalized. The sample size and evaluation of sample results shall be based on a 95% confidence level. The OAG may expand or contract sample sizes based upon historical and actual error rates for high volume performances of various Q&E requirements.
- Sample items will primarily be evaluated in terms of case processing attributes which result in *Yes or No* evaluations of each Q&E Minimum Standard and Exceptional Standard. *Yes* results represent Exceptional performance and *No* results indicates Non- exceptional performance.
- A count of sample items that are evaluated as Non-exceptional will be divided by the total sample size to calculate a *Sampled Non- exceptional Performance Rate*. This rate, subtracted from 100%, is the *Sampled Exceptional Performance Rate*.
- If the evaluation of sampled items for a Q&E measure clearly demonstrates achievement of the Exceptional Standard, then the OAG will pay the incentive amount set forth in the Quality and Efficiency Standards section of the contract.
- "Clearly demonstrates" means that the *Sampled Non- exceptional Performance Rate* has a margin of error where the upper limit is less than one-hundred percent (100%) minus the Exceptional Standard. For example:
  - 100% minus the 96% Exceptional Standard for ENFORCEMENT is a 4% *Contractual Non- exceptional Performance Rate*
  - For a given hypothetical month and county, assume there were five-hundred and sixty two cases (562) where enforcement action should have been taken or where service should have been completed during the month reviewed.
  - Further, the County has historically had about a 1% *Non- exceptional Performance Rate*.
  - Therefore, the OAG would sample eighty-one (81) sample items.
  - Assume that one (1) sample item had a *No* result of Non- exceptional performance to yield a 1.23% *Sampled Non- exceptional Performance Rate*
  - Based on a 95% confidence level, the true *Non- exceptional Performance Rate* for all ENFORCEMENT cases could range between virtually 0% and 3.64%. Because 3.64% is less than the *Contractual Non- exceptional Performance Rate*, the *Sampled Non- exceptional Performance Rate* supports OAG payment of the Quality and Efficiency Incentive.
- If the *Sampled Non- Exceptional Performance Rate* does not support OAG payment of the Quality and Efficiency incentive, then the OAG will expand its sample size up to the full population of relevant cases, until its review either supports payment or clearly demonstrates Non- Exceptional Performance.

ICSS SFY 20\_\_  
Certification of Local Expenditures

County of \_\_\_\_\_, Fiscal Year 20\_\_

From \_\_\_\_\_ To \_\_\_\_\_

Actual Local Expenditures for FY 20\_\_

Description	Total	Percent Allocation	Allocated Total
Salaries and Fringe Benefits	\$		
Travel	\$		
Operating Expenses	\$		
Indirect Cost	\$		
Other (Please Describe)	\$		
Fiscal Year Total	\$		

Verification

I DO SOLEMNLY SWEAR THAT the foregoing Financial Statement filed herewith is in all things true and correct, and fully shows all information required to be reported pursuant to Contract # 13-C0105.

\_\_\_\_\_  
Signature of Affiant

SWORN AND SUBSCRIBED BEFORE ME BY \_\_\_\_\_ this

\_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_, to certify which, witness my hand and seal.

Notary Public in and for

\_\_\_\_\_ County, Texas

**INTER-DEPARTMENTAL EQUIPMENT TRANSFER**

<b>Inventory Number</b>	<b>Description</b>	<b>Serial Number</b>	<b>Receiving Employee Location</b>

Transferred VIA  ISSS Mail  UPS  Freight Line  SSD Movers  Contract movers  Other

Interim Signature: \_\_\_\_\_ Remarks: \_\_\_\_\_

Transferring Division Code	Division Name
Receiving Division Code	Division Name

Approved for Transferring Office by:	Date:
Approved for Receiving Office by:	Date:
Property Manager's Signature:	Date:

**ACKNOWLEDGMENT OF CUSTODIANSHIP  
ATTORNEY GENERAL OF TEXAS**

I, \_\_\_\_\_, personally acknowledge that I have custody of a  
Computer (Inventory number \_\_\_\_\_, serial # \_\_\_\_\_),  
printer (Inventory number \_\_\_\_\_, serial # \_\_\_\_\_),  
fax machine (Inventory number \_\_\_\_\_, serial # \_\_\_\_\_),  
and/or other equipment (modem, tape drive, router, etc.)  
(Inventory number \_\_\_\_\_ serial # \_\_\_\_\_), on this  
\_\_\_\_ day \_\_\_\_\_ 19\_\_\_\_.

I acknowledge that the above-described equipment has been installed at \_\_\_\_\_  
\_\_\_\_\_.

I agree to accept responsibility for the security and protection of the above-described  
equipment. If any of the equipment is lost, damaged, or stolen or if any of the equipment must be  
moved from the location of installation, I will contact Property Management of the Office of  
the Attorney General. I agree to restrict the use of the above-described equipment to the  
processing of Title IV-D child support cases. I recognize that the Office of the Attorney  
General shall retain legal title to the above-described equipment. I agree to follow the  
requirements set out in 45 CFR Part 74, for the Property Management policies  
and procedures, as well as any other applicable state or federal laws or regulations.

\_\_\_\_\_  
Custodian Name (Print or Type)

\_\_\_\_\_  
Custodian Signature

Attorney General of Texas

**LOST OR STOLEN PROPERTY REPORT**  
 (TO BE COMPLETED WITHIN 24 HOURS OF DISCOVERY)

OAG SECURITY FILE  
 NO.  
 FOR SECURITY USE ONLY

Date of Report: \_\_\_\_\_

Division Name: \_\_\_\_\_ Room #: \_\_\_\_\_

Street Name: \_\_\_\_\_ City/State: \_\_\_\_\_

Location of Property: \_\_\_\_\_ Date and Time Missed: \_\_\_\_\_

Property last used or observed:

Person Property assigned to: \_

Description of lost/stolen property: \_

Name of Police Agency notified: \_\_\_\_\_ Offense Report #: \_\_\_\_\_

	Description of Property	Personal or State	OAG Inventory #	Serial Number	Cost at Time of Purchase
1					
2					
3					
4					
5					
6					

REPORT IN DETAIL: \_\_\_\_\_

Reported By: \_\_\_\_\_ Title/Dept.: \_\_\_\_\_

Address: \_\_\_\_\_ Phone #: \_\_\_\_\_

MAKE IN TRIPLICATE AND SEND ORIGINAL TO PROPERTY MANAGEMENT IN THE SUPPORT SERVICES DIVISION, ONE COPY TO THE INTERNAL SECURITY AND INVESTIGATIONS DIVISION, THEN KEEP ONE COPY FOR YOUR FILES.

**UNITED STATES INTERNAL REVENUE SERVICE REQUIREMENTS FOR THE  
SAFEGUARDING OF FEDERAL TAX INFORMATION INCLUDING FEDERAL TAX  
RETURNS AND RETURN INFORMATION**

**I. PERFORMANCE**

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's responsible employees.
- (2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract.

Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract.

Inspection or disclosure to anyone other than an officer or employee of the contractor is prohibited.

- (3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (4) No work involving returns or return information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (5) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (6) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

**II. CRIMINAL/CIVIL SANCTIONS:**

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal

to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information* and Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

### **III. INSPECTION:**

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.



ATTORNEY GENERAL OF TEXAS  
GREG ABBOTT

---

Office of the Attorney General  
Information Technology Security  
Policy Manual

Version 4.3  
April 5, 2011

Presented by: Kathleen  
DonahoJaeger CS Information  
Security Officer Mike O'Connell  
A&L Information Security Officer



## Table of Contents

1. Information Security Policy.....	4
1.1. Attorney General Policy Statement .....	4
1.2. Scope of Policy .....	4
1.3. OAG Information Security Policy Purpose & Intent.....	4
1.4. Definitions.....	4
2. Management Security Controls.....	5
2.1. State Agency Head -Attorney General .....	5
2.2. Management Responsibility.....	5
2.3. Information Resources Manager (IRM).....	5
2.4. Information Security Officers (ISO).....	5
2.5. Information Resource Owner.....	6
2.6. Information Custodian .....	7
2.7. Information Technology User.....	8
3. Operational Security Controls.....	8
3.1. Risk Management Framework.....	8
3.2. Risk Assessment .....	8
3.3. Asset Management.....	8
3.4. Disaster Recovery & Business Continuity.....	9
3.5. Outsourced Data Center Operations & Security Responsibility.....	9
4. Personnel Security Policy .....	9
4.1. Statement of Responsibility.....	9
4.2. Reporting of Security Incidents .....	9
4.3. Computer Security Incident Response Team (CSIRT).....	9
4.4. Information Security Violations .....	10
4.5. Acceptable Use of OAG Information Technology Assets.....	10
4.6. Access to OAG Information Technology Assets.....	11
4.7. User Identification .....	11
4.8. Personal Software, Hardware and Modems.....	11
4.9. Security Awareness Program.....	11
4.10. Warning Statements.....	11
4.11. Termination of Employment.....	12
4.12. Automatic Suspension / Deletion of User ID's.....	12
4.13. Positions of Special Trust .....	12
5. Technical Security Controls.....	12
5.1. System Security Policy .....	12
5.2. System Administrators.....	12
5.3. System Developers.....	12
5.4. Information Technology Asset Protection.....	13
5.5. Vendor Access to OAG Systems .....	13
5.6. Classification of Electronic Data and Assets.....	13
5.7. Data Destruction .....	13
5.8. Configuration Management .....	14
5.9. Change Management .....	14
5.10. Data Integrity .....	14

5.11. Voice/Phone Mail .....	14
5.12. E-mail.....	14
5.13. Wireless Systems .....	15
5.14. Copyright .....	15
5.15. Personal Software, Shareware and Freeware.....	15
5.16. Data Encryption .....	15
5.17. Portable and Mobile Devices.....	15
5.18. Malware Protection Software .....	15
5.19. Intrusion Detection.....	15
5.20. Internal Electronic Investigations .....	16
5.21. Screen Savers.....	16
5.22. User Passwords .....	16
5.23. Administrator Passwords .....	16
5.24. System Log On & Re-Boot.....	16
5.25. System Settings.....	16
5.26. Control of Peripherals.....	16
5.27. Security Breaches.....	17
5.28. Dial-up Access.....	17
5.29. Purchasing/Development Pre-Approval .....	17
5.30. Contract Security Provisions.....	17
5.31. System Development, Acquisition and Testing.....	17
6. Exception, Waiver and Modification.....	18
6.1. Waivers and Exceptions.....	18
6.2. Modification or Significant Changes to Procedures .....	18
6.3. Executive Management Waiver.....	18
7. Document Acceptance and Release Notice .....	19
8. References.....	20

## 1. Information Security Policy

### 1.1. Attorney General Policy Statement

The Office of the Attorney General (OAG) is committed to protecting the information resources that are entrusted to this agency. An effective data security protocol, supported by an appropriately rigorous security structure, is critical to the success of an information security program. The OAG's Information Security Officers are responsible for managing and developing the information security program, which includes identifying and resolving all at-risk information system assets, as well as supporting the operational needs of the agency.

An effective information security program encompasses many activities requiring commitment and cooperation among both employees and management of the OAG. All information resources users must be involved in the success of this strategic effort.

### 1.2. Scope of Policy

This policy applies to all OAG "information assets" that are used by or for the OAG throughout its life cycle. "Information assets" are the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.<sup>i</sup>

This policy also applies to all users of OAG information assets, and electronic data regardless of location.

To the extent there is any conflict between this policy and the Sensitive Personal Information Privacy Policy (found at <https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php>), the latter shall control.

### 1.3. OAG Information Security Policy Purpose & Intent

The purpose and intent of this policy document is to familiarize users of OAG information resources with the need to protect these resources in a prescribed manner and in accordance with appropriate standards.

### 1.4. Definitions

**Access:**

The physical or logical capability to interact with, or otherwise make use of information assets.

**Business Continuity Planning:**

The process of identifying mission critical data systems and business functions, analyzing the risks and probabilities of service disruptions and developing procedures to restore those systems and functions.

**Control:**

Any action, device, policy, procedure, technique, or other measure that improves security.

**Encryption:**

The conversion of plain text (human readable) information into a mathematical cipher or algorithm to create an electronic message that conceals the true meaning.

**Information Asset:**

The term information asset is defined in Section 1.2 of this policy.

**Information Resource Data:**

Any data electronically produced, modified, transmitted, or stored while in electronic form.

**Information Technology Asset:**

A subset of the term information asset that refers to computing hardware such as a laptop computer, desktop PC, network server, or computer software.

## 2. Management Security Controls

### 2.1. State Agency Head -Attorney General

The Attorney General, as the state agency head, is responsible for establishing and maintaining an information security and risk management program. It is the responsibility of the Attorney General to ensure that the agency's information assets are protected from the effects of damage, destruction, and unauthorized or accidental modification, access or disclosure.

### 2.2. Management Responsibility

The protection of information assets is a management responsibility. Managing information security within the OAG requires commitment and support on the part of executive, technical and program management. All managers must be involved in the security and awareness program, and be familiar with and enforce OAG policies and procedures among their staff and employees.

### 2.3. Information Resources Manager (IRM)

The IRM is the agency executive who must approve the information technology assets and services necessary to conduct the information security program, as well as use executive authority where necessary to enable the success of the information security program.

### 2.4. Information Security Officers (ISO)

A full-time ISO will oversee the Administrative and Legal Divisions (A&L), while another full-time ISO will oversee the Child Support Division (CS). The A&L ISO and CS ISO will report directly to

their respective IT Directors and indirectly to the IRM. It is the ISO's duty and responsibility to:

- Manage, develop and coordinate the development of the OAG information security program and all other information security policies, standards and procedures.
- Collaborate with IT divisions, information asset owners and executive management in the development of procedures to ensure compliance with external information security requirements.
- Develop training materials on information security for employees and all other authorized users, and collaborate with agency training staff to establish a standardized agency-wide information security training program.
- Develop and implement incident reporting and incident response processes and procedures to address any security incident/breach, violation of policy or complaint.
- Serve as the official agency point of contact for all information security inquiries and audits.
- Develop and implement an ongoing risk assessment program, including recommending methods for, and overseeing of, vulnerability detection and testing.
- Monitor security legislation, regulations, advisories, alerts and vulnerabilities, and communicate accordingly with IT divisions, data owners and executive management.
- Review agency information systems and provide written reports that identify potential security risks and recommended solutions as appropriate.
- Provide annual report to executive management on security program and risk mitigation.
- Collaborate with IT personnel, the Records Management Officer, and legal counsel to preserve data in accordance with appropriate data preservation and litigation hold procedures.

## **2.5. Information Resource Owner**

An information resource owner is defined as a person responsible for a business function and for determining controls and access to information resources supporting that business function.<sup>iii</sup> The state agency head or his or her designated representative(s) shall review and approve ownership of information resources and their associated responsibilities.<sup>iv</sup> For the OAG Information Resource Owners are typically Division Chiefs.

Where information resources are used by more than one division, the owners shall reach a consensus as to the designated owner with responsibility for the information resources and advise the A&L or CS ISO of their decision.<sup>v</sup>

The information owner or his or her designated representatives(s), with the CISO's concurrence, are responsible for and authorized to:

- Approve access to, and formally assign custody of, an information asset;
- Determine the asset's value;
- Specify data control requirements and convey them to users and custodians;
- Specify appropriate controls, based on risk assessment, to protect the agency's information resources from unauthorized modification, deletion or disclosure. Controls shall extend to information resources outsourced by the agency in accordance with the Department of Information Resources' (DIR) information security policy;
- Confirm that controls are in place to ensure the accuracy, authenticity and integrity of electronic data;
- Ensure compliance with applicable controls;
- Assign custody of information technology assets and provide appropriate authority to implement security controls and procedures; and
- Review access lists based on documented security risk management decisions.

## **2.6. Information Custodian**

An information custodian is defined as any person or group who is charged with the physical possession of information technology assets. Custodians are the technical managers that provide the facilities, controls and support services to owners and users of information. Custodians of information technology assets, including entities providing outsourced information resources services to state agencies, must:

- Implement the controls specified by the owner(s);
- Provide physical and procedural safeguards for the information assets;
- Assist owners in understanding and evaluating the cost-effectiveness of controls and monitoring;
- Administer access to the information assets; and
- Implement appropriate monitoring techniques and procedures for detecting, reporting and investigating incidents.

## **2.7. Information Technology User**

All authorized users of OAG information technology assets (including, but not limited to, OAG personnel, temporary employees, contractors, sub-contractors, auditors, consultants or agents), shall formally acknowledge that they will comply with the OAG's security policies and procedures or they shall not be granted access to the information technology assets. Each division's ISO will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to OAG information technology assets.<sup>vi</sup> Users also have the responsibility to report all suspected violations of OAG information security policies to their Division Chief and the ISO responsible for their division. The ISO will then report the suspected violation to the IRM and appropriate IT Director. (See section 3.4)

Users of OAG information technology assets shall have no expectation of privacy for information contained within or processed by an OAG information technology asset. Electronic files created, sent, received by, or stored on, OAG information technology assets that are owned, leased, administered, or otherwise under the custody and control of the OAG are not private and may be accessed by OAG IT employees at any time without knowledge of the information technology asset user or owner. Electronic file content may be accessed by appropriate personnel, including, but not limited to, information security personnel, records management personnel and legal counsel.<sup>vii</sup>

## **3. Operational Security Controls**

### **3.1. Risk Management Framework**

The OAG employs a risk-based information security strategy, which provides a method to eliminate or mitigate identified risk to an organization in order to maximize the positive effects of information security activities while minimizing costs to the organization.

### **3.2. Risk Assessment**

It is the responsibility of the ISO's to regularly assess the risk to all OAG electronic data, systems, networks and information technology operations, and report the results of the assessment to OAG executive management and other appropriate personnel.

### **3.3. Asset Management**

Management of OAG equipment including laptops, PDAs, and other IT equipment is an asset control and physical security issue and not within the scope of this Information Technology Security policy. For policy regarding those items, refer to the OAG's general Policies and Procedures, as well as the Special High-Risk Items Policy, which may be found at <https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php>.

### **3.4. Disaster Recovery & Business Continuity**

The OAG is charged with providing a comprehensive disaster recovery plan and business continuity procedure for all essential Data Center and field operations. This activity will be supported in part by the Information Security Division (ISD).

### **3.5. Outsourced Data Center Operations & Security Responsibility**

As a requirement of House Bill 1516 by the 79th Legislature, OAG information technology systems will be consolidated at the DIR Consolidated Data Centers (CDC).

While DIR and their contractor will supply much of the required services and activities to protect OAG data, systems and networks, the OAG still has responsibility for ensuring the safety of OAG data.

## **4. Personnel Security Policy**

### **4.1. Statement of Responsibility**

OAG personnel are required to sign a Statement of Responsibility acknowledging that they agree to comply with all applicable information security policies, protocols and procedures as set forth in the OAG Information Security Policy Manual. This statement of responsibility will remain a part of the employee's file.

### **4.2. Reporting of Security Incidents**

A security incident is defined as an event which results, or may result in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

Employees and all other users shall immediately report all actual or suspected security incidents to their Division Chief and the appropriate ISO. The ISO will promptly notify the IRM and appropriate IT Director of the actual or suspected security incident. The ISO shall report any security incidents that affect critical systems and/or that could be propagated to other state systems outside the OAG to DIR within twenty-four hours.

### **4.3. Computer Security Incident Response Team (CSIRT)**

The OAG Computer Security Incident Response Team (CSIRT) is responsible for the detection, triage, response, communication and management of all information security incidents. The CSIRT will:

- Provide a single point of contact at OAG for managing all reported OAG information resource electronic attacks, whether suspected or actual;
- Identify and analyze what has occurred, including impact and threat;
- Research and recommend solutions and mitigation strategies;



- Share response options, recommendations, incident information and lessons learned with appropriate entities; and
- Coordinate response efforts.

The CSIRT is comprised of three separate groups that include both permanent IT personnel certified in CSIRT operations, and ad hoc personnel based on the nature of the incident:

1. Management Group:
  - Membership includes: The affected division's ISO and IT Director.
  - May include: IRM.
  - Responsibilities: Manage CSIRT operations (ISO), manage overall incident response, document activities, and produce appropriate reports. Also responsible to communicate internally to executive management.
2. Technology Group:
  - Membership includes: Director of impacted network and Director of impacted infrastructure and/or application.
  - May include subject matter experts (SMEs) from specific disciplines.
  - Responsibilities: Analyze event, recommend possible courses of action, and coordinate selected response.
3. Legal Group:
  - Membership includes: Attorney(s) from, or assigned by, the General Counsel Division, and the Records Management Officer.
  - May include: Law enforcement investigators.
  - Responsibilities: Produce draft of external communications; function as team's legal representative for guidance regarding evidence gathering and other possible legal issues and activities.

#### **4.4. Information Security Violations**

Violations of information security policy could result in a security breach. For this reason, violations of information security policy will be investigated by the appropriate IT personnel. If the violation is found to be deliberate in nature, an official Information Security Violation Report (ISVR) will be issued by the appropriate ISO, with an informational copy provided to the Records Management Officer. Additionally, such violations will be reported to the employee's Division Chief and the Human Resources Director for corrective action. Any corrective action involving use of information technology resources must be documented and reviewed by the appropriate ISO prior to implementation.

#### **4.5. Acceptable Use of OAG Information Technology Assets**

State information technology assets will be used primarily for official State purposes. Software for browsing the Internet is provided to authorized users to conduct official State business. Compliance with this policy will be electronically monitored. Any personal use must be in accordance with the OAG's policy regarding the Unauthorized Use of Government Time, Property, Services, and Facilities, found at

<https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php>.

Violations may result in disciplinary action, up to and including termination of employment. The unauthorized use of OAG information assets will be considered as a relevant factor in evaluating the performance of OAG employees.

#### **4.6. Access to OAG Information Technology Assets**

Access to OAG information technology assets must be strictly controlled and monitored to provide users with only the minimum level of system access necessary to allow them to perform assigned business tasks. When access by the user requires the use of a password, or other security measure, those security measures must be kept confidential by the intended user. Remote access to OAG information systems and assets must be accomplished only through the use of an OAG-approved remote access software application.

#### **4.7. User Identification**

Except for public users of systems where such access is authorized by the appropriate ISO or other appropriate IT personnel, each system user shall be assigned a unique personal identifier or user identification (User ID) to allow system access.

#### **4.8. Personal Software, Hardware and Modems**

Personal software may not be loaded onto any OAG computer, nor may personally-owned hardware, including modems and wireless routers, be connected to OAG information systems. Any hardware or software required for a business purpose of the agency must be approved for use by the appropriate ISO and must be obtained through the appropriate ITS Division.

#### **4.9. Security Awareness Program**

The OAG will provide an ongoing Information Security Awareness training program to educate employees and all other personnel with access to OAG data and information systems about data security and the protection of OAG information resources. This training will include the establishment of security awareness and familiarization with OAG security policies and procedures through both New Employee Orientation and ongoing refresher training.

#### **4.10. Warning Statements**

System identification screens will be provided at the time of initial logon to the mainframe or LAN/WAN. These screens will provide the following warning statements:

- Unauthorized use is prohibited.
- Usage may be subject to security testing and monitoring.
- Misuse may be subject to disciplinary action.
- No expectation of privacy is to be anticipated by the user.

#### **4.11. Termination of Employment**

Computer user identifications (User IDs) for employees that have voluntarily terminated employment with the OAG must be removed from the computer system immediately following termination. For involuntary terminations, the ID should be removed prior to, or at the same time the employee is notified of the termination in order to protect OAG data and information assets.

#### **4.12. Automatic Suspension / Deletion of User ID's**

Mainframe, LAN and Remote Access User IDs will be monitored for usage to protect system security, and any unused user IDs will be subject to automatic suspension after 30 days, and deletion after 60 days without notice to the user, unless an exception has been approved in accordance with this policy.

#### **4.13. Positions of Special Trust**

The ISOs will establish procedures for reviewing information resource functions to determine which positions require special trust or responsibilities. These include, but are not limited to:

- Network and system administrators;
- Users with access to information systems that process or contain federal tax information;
- Users with access to child support systems and data that may include federal tax information;
- Users with access to financial and accounting systems or networks;
- Any user with agency-wide access to data and information systems; and
- Any user required to undergo a background check as a prerequisite to employment or grant of system access.

## **5. Technical Security Controls**

### **5.1. System Security Policy**

The following policies cover specific issues as they relate to the security of information systems and data within the OAG, and are governed by the procedures outlined in the OAG Information Security Procedures Manual.

### **5.2. System Administrators**

System administrators are responsible for adding, removing or modifying user accounts as employees change roles within the agency. This activity must be accomplished in a timely manner to ensure only authorized personnel have access to OAG systems and information. Changes to user accounts may be subject to independent audit review.

### **5.3. System Developers**

All production software development and software maintenance activities performed by in-house staff must adhere to agency security policies, standards, procedures, and other systems development conventions including appropriate testing, training and documentation.

#### **5.4. Information Technology Asset Protection**

OAG data and information technology assets will be protected from unauthorized access, use, modification or destruction through the deployment of protective measures. The design, acquisition and use of all protective measures must be reviewed and approved by the appropriate ISO.

#### **5.5. Vendor Access to OAG Systems**

Access to OAG systems and data by vendors (including contractors, sub-contractors, auditors, consultants or agents) must be appropriately controlled depending on the work to be performed, sensitivity levels of the data involved, work location, and other relevant considerations. All requests for vendor access must be coordinated with and approved by the appropriate IT department and ISO prior to access being granted.

#### **5.6. Classification of Electronic Data and Assets**

OAG electronic data and the information technology assets used to process, transmit, and store it should be assigned an appropriate classification level to assist in the proper safeguarding of the data. As higher classification levels require the agency to incur greater costs in order to safeguard data, care should be taken to accurately classify assets. Assets of varying classifications that are co-mingled in a single database or file system shall be classified at the highest level of the information contained in the data.

For the limited purposes of this policy, the OAG has two classifications of electronic data:

- **CONFIDENTIAL AND SENSITIVE** -This classification includes data that may be deemed confidential or protected by Texas or federal laws and/or administrative rules, and sensitive information, which if subject to a security breach, could compromise the agency's business functions or the privacy or security of agency employees, clients, or partners. Information in this category may only be provided to external parties in accordance with OAG policies and procedures.
- **UNCLASSIFIED** -This refers to all data that does not meet the requirements for **CONFIDENTIAL AND SENSITIVE** as described herein, as designated by the originating source of the data and/or the originator of any derivative data with guidance from 1 TAC § 202.1(3); DIR Classification Guidance, and any other applicable regulation or law.
- The default classification for all electronic data is **CONFIDENTIAL AND SENSITIVE**.

#### **5.7. Data Destruction**

OAG data should only be destroyed in accordance with the applicable records retention schedule, or upon the receipt of proper authorization from the State Library and Archives Commission. OAG data contained on magnetic or optical media must be removed from the media prior to the media being transferred out of the control of the authorized user, or the media must be physically destroyed in accordance with the appropriate document destruction guidelines applicable to that information.

## **5.8. Configuration Management**

Configuration management (CM) is the process of managing the effects of changes or differences in configurations of an information system or network through the implementation of strict protocols and testing in order to reduce the risk of changes resulting in a compromise to data security, confidentiality, integrity, or availability. All systems will be configured and maintained only in accordance with approved IT and Information Security configuration management (CM) guidelines.

## **5.9. Change Management**

Change management refers to the safeguards and procedures established for making modifications to OAG systems and networks. All such modifications must be processed through the appropriate change control procedure, with any OAG systems residing at a Consolidated Data Center (CDC) additionally being subject to the DIR and its contractor change management process.

## **5.10. Data Integrity**

Data integrity refers to ensuring that data remains complete and unchanged during the course of any electronic processing, transfer, storage, or retrieval. To promote data integrity, individual users of OAG information assets must follow data integrity procedures applicable to their level of user access to OAG data, and take adequate precautions to safeguard against the loss of OAG data, including but not limited to:

- Performing regular backups of OAG data as may be appropriate;
- Taking physical and procedural safeguards to avoid the accidental loss, destruction or unauthorized modification of OAG data;
- Ensuring proper and routine use of virus protection software/anti-malware; and
- Coordinating with and seeking assistance from IT personnel as may be appropriate to safeguard OAG data.

## **5.11. Voice/Phone Mail**

The OAG's voice or phone mail systems use agency information assets. Accordingly, each user is responsible for ensuring that use of these services is in compliance with applicable law, policy and procedures. All requests for changes, modifications, or termination of voicemail services must be initiated through the ITS Division.

## **5.12. E-mail**

Electronic mail (e-mail) is a form of communication that uses agency information assets. All use of e-mail must be in accordance with OAG policies and procedures regarding the use of information assets.

Upon the OAG's implementation of an agency-approved email encryption process, employees may not send CONFIDENTIAL AND SENSITIVE OAG data in the body of an email or as an email attachment across unsecured connections such as the Internet, unless it is encrypted using a process approved by both the appropriate IT Director and ISO.

### **5.13. Wireless Systems**

Wireless networks or routers may not be used without the prior authorization of both the appropriate IT Director and ISO. All wireless connectivity (Wi-Fi) to OAG networks must be in accordance with current IT architectural direction, Information Technology Security Policy, and OAG policies and procedures relating to the use of mobile telecommunications devices.

### **5.14. Copyright**

Generally, the reproduction of copyrighted information is a violation of federal law. Therefore, OAG information assets should not be used to reproduce copyrighted information. Unauthorized copies of software shall not be loaded or executed on OAG information technology assets. Regular audits will be conducted to search for unauthorized software installed on machines.

### **5.15. Personal Software, Shareware and Freeware**

Personal software, shareware and freeware may not be loaded or otherwise used on OAG systems unless there is a business necessity for the use of such programs, and their installation and use is specifically approved by both the appropriate IT Director and ISO.

### **5.16. Data Encryption**

All OAG laptops must have encrypted hard drives to safeguard data in the event the device is lost or stolen. Those divisions who choose to employ data encryption for transmission or storage of CONFIDENTIAL AND SENSITIVE data shall adopt the 256 bit Advanced Encryption Standard (AES), or 128 bit Single Sockets Layer (SSL/TLS) as a minimum. No encryption will be used without the prior approval of both the appropriate IT Director and ISO.

### **5.17. Portable and Mobile Devices**

All laptops and other mobile telecommunications devices (PDAs, network capable cell phones, BlackBerry's, etc.) must be approved for use and supplied by the appropriate ITS Division. Only OAG laptops installed with full-disk encryption, anti-malware safeguards, and secure connectivity are authorized for use with OAG data and networks.

### **5.18. Malware Protection Software**

All workstations and laptops must use approved malware protection software and configurations, regardless of whether they are connected to OAG networks or are used as a standalone device. Additionally, each file server attached to the OAG network and each e-mail gateway must utilize OAG IT-approved e-mail malware protection software and/or hardware. Users shall not alter, disable, bypass, or adjust any settings or configurations for OAG malware protection software in any manner.

### **5.19. Intrusion Detection**

Intrusion detection techniques will be deployed wherever possible in order to safeguard against unauthorized attempts to access, manipulate, or disable OAG networks. Intrusion detection activities may be conducted only by specially-trained personnel within the OAG using techniques approved by the appropriate ISO.

## **5.20. Internal Electronic Investigations**

All internal electronic investigations must be authorized by, and conducted under the supervision of, the appropriate ISO unless otherwise approved by the First Assistant Attorney General. No other investigation is authorized on OAG systems or networks. Any unauthorized electronic investigation or monitoring discovered on OAG systems or networks will be reviewed by the Information Security Division and may result in disciplinary action up to and including termination of employment.

## **5.21. Screen Savers**

To reduce the likelihood of unauthorized access to OAG data, systems and networks, all OAG workstations, including laptop computers, must be configured to activate password-protected screensavers after no more than fifteen minutes of user inactivity. An employee should not leave his or her workstation unless the password-protected screensaver has been activated or, if possible, the workstation has been secured by a locked door.

## **5.22. User Passwords**

Systems that use passwords shall follow the standards on password usage prescribed by DIR found at <http://www2.dir.state.tx.us/security/policy/Pages/policy.aspx>. This document specifies minimum criteria and provides guidance for selecting additional password security criteria. Disclosure of an individual's password or use of an unauthorized password or access device may result in disciplinary action up to and including termination of employment.

## **5.23. Administrator Passwords**

All system administrators will maintain and use both a standard user password and a system administrator password ("super user" password). The system administrator password will be used only for system administrator activities. All common applications and system activities (email, calendar, etc.) must be accessed by the system administrator only with their standard user password.

## **5.24. System Log On & Re-Boot**

All OAG workstations, including laptop computers, must be connected to the OAG network at least once weekly in order to receive appropriate application updates and security patches. Additionally, all systems must be re-booted (shut down and restarted) at least once a week to ensure these updates and patches are installed appropriately.

## **5.25. System Settings**

All OAG systems are specifically configured to ensure that users have the appropriate ability to perform assigned tasks. Users shall not modify, change or attempt to change any system settings. If additional user access, permissions or system setting changes are required, then a request for the modification must be approved by the user's manager and submitted to the appropriate IT Division for handling.

## **5.26. Control of Peripherals**

A peripheral device is any device attached to a computer in order to expand its functionality, such as USB flash drives, CD burners, or PCMCIA card slots. The ability to use peripheral

devices may be controlled on some OAG systems; users are not authorized and should not attempt to change control settings in order to use peripheral devices on these systems. Adding or deleting peripherals on these systems may only be accomplished by IT personnel.

### **5.27. Security Breaches**

A security breach is defined as any event which results in loss, disclosure, unauthorized modification, or destruction of information resources. Users shall immediately report all actual or suspected security breaches to their Division Chief and the ISO responsible for their division. The responsible ISO will promptly report the suspected or actual security breach to the appropriate IT Director and IRM. Depending on the nature of the information involved, additional procedures may be required in accordance with the Sensitive Personal Information Privacy Policy.

### **5.28. Dial-up Access**

For dial-up access to OAG systems other than access authorized for the public, information security protocols shall be employed to positively and uniquely identify authorized users and authenticate user access to the requested system. All modems used for dial-up access to OAG systems must be authorized by the appropriate IT Director and ISO.

### **5.29. Purchasing/Development Pre-Approval**

All OAG purchases, acquisitions, or developments of information technology services, equipment or software must be reviewed and pre-approved by the appropriate ISO to determine whether the purchase may negatively impact OAG information technology security. All purchases of information technology security products, or products with information technology security functionality or impact, must be approved by the IRM and appropriate ISO prior to the issuance of a purchase order.

### **5.30. Contract Security Provisions**

All third-party contracts must contain appropriate language to ensure the security of OAG information to which the third-party may have access, even if such access is limited to encrypted data. This language must state in clear and unambiguous terms the security requirements placed on the third-party involved, and their responsibilities for security under the contract. It must also clearly state OAG's authority to audit their security procedures for appropriateness during the length of the contract.<sup>xii</sup>

All contracts to which the OAG is a party and that affect OAG information technology security must be reviewed and approved by the appropriate ISO prior to execution in order to ensure that appropriate security controls are included.

### **5.31. System Development, Acquisition and Testing**

Data and network security requirements must be considered and addressed in all phases of the development or acquisition of new information processing systems. Before being placed into use, all new systems must be properly tested in order to ensure compatibility with OAG information systems and the OAG computing environment. During system testing, test functions shall be kept either physically or logically separate from production functions in



order to safeguard OAG data and information technology systems.

## **6. Exception, Waiver and Modification**

### **6.1. Waivers and Exceptions**

Waivers and exceptions to the existing information security policies and procedures are strongly discouraged because they may pose an unacceptable risk to protected OAG data and systems. Prior to implementation, all exceptions or waivers of existing security policies or procedures must be reviewed and approved by the IRM, appropriate IT Director, appropriate ISO, and reported to the Records Management Officer.

- A waiver is a variance of a control standard that is limited to a specific period of time and to a specific system in order to allow IT personnel to perform an approved change or modification to OAG systems.
- An exception is an indefinite variance from a control standard supported by a valid and ongoing business justification.

### **6.2. Modification or Significant Changes to Procedures**

All changes in the procedures to protect OAG IT systems and data must be reviewed by the appropriate IT Director and approved by the appropriate ISO prior to implementation. If immediate changes to procedures are required to meet an emergency situation, A&L and/or CS ISO, and the Records Management Officer must be informed as soon as possible thereafter.

### **6.3. Executive Management Waiver**

Notwithstanding any provisions to the contrary contained herein, waivers, exceptions and modifications to the information security policies and procedures may be authorized in writing at the discretion of the First Assistant Attorney General.

Office of the Attorney General

## 7. Document Acceptance and Release Notice

This is Version 4.2 of the OAG Information Security Division Security Policy Manual.

The OAG Information Security Division Security Policy Manual is a managed document. Changes will be issued only as a complete replacement document. Recipients should remove superseded versions from circulation. This document is authorized for release after all signatures have been obtained.

Please submit all requests for changes to the owner/author of this document.

OWNER:  DATE: April 5, 2011  
Mike O'Connell, A&L Information Security Officer

OWNER:  DATE: April 5, 2011  
Kathleen Donaho-Jaeger, CSD Information Security Officer

EXECUTIVE SPONSOR:  DATE: April 5, 2011  
Diane B. Smith, Deputy for Administration and Information Resources Manager

## 8. References

Tex. Gov't Code § 2054.003(7).

\*1 TAC § 202.20.

"1 TAC § 202.1

"1 TAC § 202.21.

'1 TAC § 202.21.

"1 TAC § 202.21.

"1 TAC § 202.27.

viii *See* , 1 TAC Chapter 202.

*generally*  
"1 TAC § 202.21.

'1 TAC § 202.1.

"1 TAC § 202.26.

"1 TAC § 202.25(6)(B).



OFFICE of the ATTORNEY GENERAL  
G R E G A B B O T T  
CHILD SUPPORT DIVISION

**AUTOMATED COMPUTER SYSTEM ACCESS – STATEMENT OF RESPONSIBILITY**

Name:	Agency Employed By:
Position:	Work Location (Address, City, Country):
Phone:	
FAX:	

If given access to the automated computer system maintained by the Office of the Attorney General of Texas, I agree to the following:

1. All information maintained in the files and records of the Office of the Attorney General of Texas (OAG), Child Support Division are privileged and confidential.
2. Information that I obtain about anyone while using the computer system of the OAG must be held in strictest confidence and may not be disclosed except as used exclusively for purposes directly connected with the administration of programs under Titles IV-A, IV-D, IV-E and XIX of the federal Social Security Act and in accordance with the OAG Confidentiality Policy and Procedures.
3. Only authorized personnel may view, add, modify and/or delete information.
4. I may not perform any work, review, update or otherwise act to obtain information about my own, or any relative's, friend's, or business associate's child support case, even if the case is closed.
5. The computer password(s) I receive or devise are confidential, and must not be disclosed to anyone.
6. I am responsible for computer transactions performed through misuse of my password(s).
7. Use of a password not issued or devised specifically for me is expressly prohibited and is a violation of Texas and United States law.
8. I will not load unauthorized software, personal computer programs, shareware or freeware of any kind onto the OAG computer equipment.
9. Copyrighted material, including commercial computer software, which may be made available to me for use by the OAG is protected by copyright laws and is not to be copied for any reason without written permission from the owner of the copyright and the OAG.
10. United States federal tax return or return information may not be disclosed to any individual or agency.
11. It is unlawful to offer or receive anything of value in exchange for United States federal tax return or return information.

**CIVIL AND CRIMINAL PENALTIES**

I acknowledge that if I fail to observe this agreement, the following civil and criminal penalties apply:

1. A violation will be reported to appropriate personnel for disciplinary action, including termination and referral for prosecution.
2. Failure to observe the above conditions may constitute a "breach of computer security" as defined in the TEXAS PENAL CODE, CHAPTER 33, Section 33.02 (b), and that such an offense may be classified as a felony. Similar United States federal statutes may also be applicable.
3. Unauthorized disclosure or exchange of federal tax information is punishable by fine up to \$5,000, or imprisonment up to 5 years, or both, under United States Internal Revenue Code 7213 and 7213 A
4. Accessing federal tax information without a "need-to-know" is a federal misdemeanor punishable by not more than one year imprisonment, or a \$1000 fine or both, plus costs of prosecution under 7213 A, United States Internal Revenue Code.
5. I may be civilly liable for damages of not less than \$1000 per violation for unauthorized disclosure of federal tax information, together with costs of prosecution under Section 7431 of the United States Internal Revenue Code.

SIGNATURE: \_\_\_\_\_ DATE: \_\_\_\_\_

FAX completed form to HelpDesk at FAX number 512-460-6027

# WARNING

## DISCLOSURE LIMITATIONS

Unauthorized disclosure, printing, or publishing of any Federal return or return information, or any information therefrom, is punishable by fine up to \$5,000 or imprisonment up to 5 years, or both, together with costs of prosecution. See Sec. 7213 of the Internal Revenue Code (IRC) and 18 U.S.C. Sec. 1905. A person authorized to access IRS return or return information can be prosecuted under the federal "Anti- Browsing" Law, see IRC Sec, 7213A, if the information was accessed without a need to know. The offense constitutes a federal misdemeanor punishable by not more than 1 year in prison, or a \$1,000 fine, or both, plus cost of prosecution. In addition, IRC Sec. 7431 provides for civil damages of not less than \$1,000 per violation for unauthorized disclosure of such information, together with costs of prosecution.

It is unlawful for any person willfully to offer any item of material value in exchange for any return or return information and to receive as a result of such solicitation any such return or return information. Such action is punishable by fine up to \$5,000 or imprisonment up to 5 years, or both, together with costs of prosecution. See Sec, 7213 of the IRC and 18 U.S.C. Sec. 1905. Section 6103 (1) (8) of the IRC permits the SSA to disclose tax return information to IV-D agencies subject to the same restrictions on disclosure above.

I acknowledge that I am aware of the above civil and criminal liabilities.

Name (please print) \_\_\_\_\_

Date \_\_\_\_\_

Signature \_\_\_\_\_

SSN \_\_\_\_\_

Please check the appropriate box below that indicates your current Employment Status or your affiliation with the Attorney General of Texas agency:

- |   |   |
|---|---|
| <input type="checkbox"/> Child Support Full-Time Equivalent (FTE) Staff | <input type="checkbox"/> External Entity Staff (e.g., DHS, TWC, County, etc.) |
| <input type="checkbox"/> Child Support Part-Time Staff                  | <input type="checkbox"/> Intern   |
| <input type="checkbox"/> Contractor/Vendor Staff                        | <input type="checkbox"/> Temporary Staff                                      |
| <input type="checkbox"/> County Enforcement Staff                       | <input type="checkbox"/> Volunteer  |

**For Field staff, please follow your local or Regional procedures when submitting this form for processing. For State Office staff, please forward completed form to: Brenda Staehr, Child Support Division, Procedures and Training Section, Mail Code 053, P.O. Box 12017, Austin, Texas 78711-2017.**

# **ITS Department**

## **Security Incident Response Plan**

### **For OAG Data**

Version: Final 01.01.01

Prepared by:

Shannon Clyde Information  
Security Manager

Last Update: June 04, 2012

## A. REVISION HISTORY

<b>Contributors</b>	<b>Date</b>	<b>Reason For Changes</b>	<b>Version</b>
Shannon Clyde, ISM	November 14, 2007	Approved final version	01.00.00
Judy Pittsford, acting CIO	November 14, 2007	Approved final version	01.00.00
Shannon Clyde	July 12, 2010	Replaced David Stanton with Chris Eckert. Honorifics added. Cell phone numbers added for Chris and Shannon. Corrected A. Broussard email address; Corrected OAG titles and honorifics; Replaced Cecelia Burk with Scot Doyal. Validated OAG contacts	01.00.01
Shannon Clyde	July 12, 2010	Minor typo corrections to contacts.	01.00.02
Shannon Clyde, ITS	July 12, 2010	Approved update	01.01.00
Scot Doyal, DRO	July 12, 2010	Approved update by mail	01.01.00
Joe Harlow, CIO	July 13, 2010	Approved update	01.01.00
Shannon Clyde, ISM	June 04, 2012	Updated contact information	01.01.01

## B. TABLE OF CONTENTS

A. REVISION HISTORY .....	2
B. TABLE OF CONTENTS .....	3
C. INTRODUCTION .....	4
1.0 Objectives and Scope .....	4
2.0 Audience .....	4
3.0 Keywords Defining Requirements .....	4
4.0 Requirement Priorities .....	5
5.0 Document Change Management .....	5
D. INCIDENT RESPONSE CONTACT INFORMATION .....	6
1.0 Office of Attorney General (OAG) Contacts .....	6
2.0 Travis County Contacts.....	6
E. OAG DATA INCIDENT MANAGEMENT REQUIREMENTS .....	7
1.0 General Requirements .....	7
2.0 Responsibility for Notifications and Reports .....	7
3.0 Notification Requirements .....	7
4.0 Reporting Requirements .....	8



## C. INTRODUCTION

### 1.0 Objectives and Scope

The Travis County ("County") Information and Telecommunications Systems Department (ITS) Security Incident Response Plan for Office of the Attorney General (OAG) Data supplements the Travis County ITS Department Incident Response Standards and Procedures.

This Security Incident Response Plan is intended to provide the specific requirements that must be met to comply with ICSS Contract # 13-C0105.

### 2.0 Audience

Those who need to participate in the ITS Incident Response efforts involving OAG Data including Community Supervision staff, ITS Department staff and those who need to interact with the incident management efforts involving OAG Data.

### 3.0 Keywords Defining Requirements

The following keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are utilized within this document to indicate requirement levels and are to be interpreted as described below:

**SHALL:** This word, or the terms "REQUIRED" or "MUST", means that the definition is an absolute requirement of the specification.

**SHALL NOT:** This phrase, or the phrase "MUST NOT", means that the definition is an absolute prohibition of the specification.

**SHOULD:** This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

**SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications must be understood and the case carefully weighed before implementing any behavior described with this label.

**MAY:** This word, or the adjective "OPTIONAL", means that an item is truly optional. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation that does

include the option, though perhaps with reduced functionality. In the same vein, an implementation, which does include a particular option, **MUST** be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature the option provides.)

#### **4.0 Requirement Priorities**

Requirements that use the key word **MUST** or **SHALL** have the highest priority.

Those described as **RECOMMENDED**, as indicated by the use of the key word **SHOULD**, have a secondary priority to those requirements using the key words **SHALL** or **MUST**.

Those described as **OPTIONAL**, as indicated by the use of the key word **MAY**, have a tertiary priority. All first priority requirements represent core functionality critical to the project and must be met.

As many secondary priority requirements should be met if allotted time, human resources and funding permit.

Tertiary priorities should be completed only after all first and secondary priorities have been met.

#### **5.0 Document Change Management**

Requests for changes to this document should be made in writing to the Information Security Manager or the Chief Information Officer.

## D. INCIDENT RESPONSE CONTACT INFORMATION

### 1.0 Office of Attorney General (OAG) Contacts

<b>Role/Position</b>	<b>Name</b>	<b>Phone Number</b>	<b>Email address</b>
Chief of Information Security Officer	Willie Harvey	512-460-6764	<a href="mailto:Willie.Harvey@texasattorneygeneral.gov">Willie.Harvey@texasattorneygeneral.gov</a>
ICSS Contract Manager; County Contracts Manager, Child Support Division	Karla McDougal	512-460-6167	Karla.McDougal@texasattorneygeneral.gov

### 2.0 Travis County Contacts

<b>Position</b>	<b>Name</b>	<b>Phone Number</b>	<b>Email address</b>
Chief Information Officer	Mr. Joe Harlow	512-854-9372	<a href="mailto:Joe.Harlow@co.travis.tx.us">Joe.Harlow@co.travis.tx.us</a>
Information Security Manager ITS Department	Mr. Shannon Clyde	Office: 512-854-7846 Cell: 512-589-0740	Shannon.Clyde@co.travis.tx.us
ITS Department Help Desk	Not Applicable	512-854-9175	ITS.Helpdesk@co.travis.tx.us
ICSS Contract Manager; Director of Domestic Relations Office	Mr. Scot Doyal	512-854-9674	Scot.Doyal@co.travis.tx.us

## **E. OAG DATA INCIDENT MANAGEMENT REQUIREMENTS**

### **1.0 General Requirements**

County shall respond to security incidents involving OAG Data in accordance with ITS Department Incident Management Standards and Procedures and specific OAG requirements as stated within this Incident Response Plan for OAG Data.

### **2.0 Responsibility for Notifications and Reports**

The Information Security Officer or designate is responsible for the data collection, document creation, and delivering of the required notices and reports identified within this plan.

### **3.0 Notification Requirements**

#### **3.1. Initial Incident Notification to OAG**

##### **3.1.1. OAG Notification Time Frame, Recipients, Method**

The OAG CISO and the OAG Contract Manager must be notified by telephone and electronic mail *within one (1) hour of determination that OAG Data is involved in the incident.*

##### **3.1.2. OAG Notification Content**

Content of the notification must include:

- Notice of incident
- Description of affected systems and networks
- Initial damage assessment
- Potential scope of the incident
- Containment/Eradication/Recovery steps taken to date
- Any changes in County contact information

## 4.0 Reporting Requirements

### 4.1. Initial Written Report to OAG

#### 4.1.1. Initial OAG Report Time Frame, Recipients, Method

The Information Security Manager or designate must provide a written report to the OAG CISO and the OAG Contract Manager by electronic mail *within twenty-four (24) hours of determination that OAG Data is involved in the incident.*

#### 4.1.2. Report Content

- Disclosure of all information relating to the incident
- Results of preliminary damage analysis
- Time, nature of incident; mitigation efforts; corrective actions; estimated recovery time

### 4.2. Daily Status Report to OAG:

#### 4.2.1. Daily OAG Status Report Time Frame, Recipients, Method

The Information Security Manager or designate must provide a *daily* oral status report to the OAG CISO or designate and an electronic mail message follow up to the OAG CISO and the OAG Contract Manager

#### 4.2.2. Report Content

- Current damage analysis
- Status of containment, eradication, recovery efforts

### 4.3. Final Report to OAG:

#### 4.3.1. Final OAG Report Time Frame, Recipients, Method

The Information Security Manager or designate must provide a final written report by electronic mail to the OAG CISO and the OAG Contract Manager *within five (5) days of the completion of the final damage analysis and the completion of the eradication/recovery phases but prior to incident closure.*

#### 4.3.2. Report Content

- Cause of security incident
- Nature of security incident
- Description of cure, effective date, description of how cure protects from recurrence
- Certification Statement: County's security program is operating with the effectiveness required to assure that the confidentiality and integrity of OAG Data are protected

**CERTIFICATION REGARDING LOBBYING  
DEPARTMENT OF HEALTH AND HUMAN SERVICES  
ADMINISTRATION FOR CHILDREN AND FAMILIES**

**PROGRAM: CHILD SUPPORT ENFORCEMENT PROGRAM PURSUANT TO TITLE IV-D  
OF THE SOCIAL SECURITY ACT OF 1935 AS ADMINISTERED BY THE OFFICE OF THE  
ATTORNEY GENERAL OF TEXAS**

**PERIOD: September 1, 2012 - August 31, 2014**

**Certification for Contracts, Grants, Loans and Cooperative Agreements**

The undersigned certifies, to the best of his or her knowledge and belief, that:

- (1) No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an office or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Agency/Organization

\_\_\_\_\_  
Date



ATTORNEY GENERAL OF TEXAS  
GREG ABBOTT  
CHILD SUPPORT DIVISION

## WARNING

### DISCLOSURE LIMITATIONS

**It is unlawful for any person willfully to disclose, print, or publish, except as authorized, any Federal return or return information, or any information therefrom. Such action is punishable by fine up to \$5,000 or imprisonment up to 5 years, or both, together with costs of prosecution. See section 7213 of the Internal Revenue Code. In addition Internal Revenue Code section 7431 provides for civil damages of not less than \$1000 per violation for knowing or negligent disclosure of such information plus in the case of a willful disclosure or a disclosure which is the result of gross negligence, punitive damages, plus the costs of the action.**

**It is unlawful for any person willfully to offer any item of material value in exchange for any return or return information and to receive as a result of such solicitation any such return or return information. Such action is punishable by fine up to \$5000 or imprisonment up to 5 years, or both, together with costs of prosecution. See section 7213 of the Internal Revenue Code.**

**It is unlawful for any person willfully to inspect, except as authorized, any Federal return or return information. Such action is punishable by a fine up to \$1000 or imprisonment up to 1 year, or both, together with the costs of prosecution. See section 7213A of the Internal Revenue Code. In addition Internal Revenue Code section 7431 provides for civil damages of not less than \$1000 per violation for knowing or negligent inspection of such information plus in the case of a willful inspection or an inspection which is the result of gross negligence, punitive damages, plus the costs of the action.**



**TRAVIS COUNTY IV-D ENFORCEMENT OFFICE TERMINATION  
TRANSITION PLAN  
OAG Contract Number 13-C0105**

Pursuant to State of Texas Contract Number 13-C0105, the Attorney General of Texas (OAG) and the County of Travis agree to follow the transition plan described below should the contract be terminated. Either party shall provide to the other written notice of intent to terminate at least ninety (90) calendar days prior to the effective date of the termination. In addition, County will continue to provide services under this agreement, if requested by the OAG, for an additional thirty (30) calendar days beyond the termination effective date. In such event, the original termination effective date shall be extended pursuant to this provision.

Travis County and the OAG agree to follow the plan described below if Contract 13-C0105 is terminated:

- 1) **Effective date of termination.** Effective date of termination will fall on the first working day of the week.
- 2) **Transfer of case files**
  - a) County will make the 1010 Lavaca Street Building and the Travis County ICSS case file areas available to OAG staff on the weekend preceding the effective date of termination agreed to by County and the OAG.
  - b) County will allow the OAG to remove all Travis County ICSS case files from the 1010 Lavaca Street Building in their existing file folders. File folders and all case file contents will be recovered at no cost to the OAG.
- 3) **Notification of Customers**
  - a) During and after the transition period, County will be responsible for notifying walk-in clients of the closure of the County office and the transfer of case enforcement responsibilities to the OAG.
  - b) The OAG will be responsible for notifying in writing all custodial parents on former County Full Service Enforcement Office cases of the transfer of the CP's case to a specified OAG field office in Travis County.
- 4) **Return of OAG equipment.** All OAG equipment provided to County under the contract will be removed by OAG staff during the first week that all Travis County ICSS cases have been transferred to the OAG.
- 5) **Interim Measures**
  - a) New cases opened on TXCSES in the Travis County ICSS Office during the transition period will be processed through Case Initiation by County staff, then transferred within two business days to the designated OAG field office.

- b) During the transition period, all existing ICSS cases will continue to be serviced by County according to OAG policy and procedures until the transfer of all case files is complete.
- 6) **Reimbursement for last month of operation.** The OAG shall reimburse County on a pro-rata basis for services provided during the final month of the contract if the contract termination effective date does not fall on the last day of the month. Reimbursement shall include new cases worked through the Case Initiation process by County, then transferred within 2 business days to the designated OAG field office.
- 7) **New case referral decision.** County and the OAG must agree if new child support obligations established after the effective date of termination will continue to be referred for Title IV-D services under the operation of the existing Local Rule.
- a) **Option 1--Terminate new case referral process.** If County decides that its new county child support obligations will no longer be referred for IV-D services, County must:
- i) Revoke the existing Local Rule effective on the agreed-upon termination effective date.
  - ii) Post advance public notice of the effective date of the revocation of the Local Rule in accordance with state law.
- b) **Option 2--Continue new case referral process.** If County decides to continue to refer new child support obligations for Title IV-D services, the OAG and County must agree on the referral method a minimum of 30 calendar days in advance of the effective termination date of the contract:
- i) **Case Referral Option 1—Automated referral by daily electronic file.** County may decide to transfer new case information to the OAG via generation and transmission of a daily electronic file.
  - ii) **Case Referral Option 2—Access by OAG to County's Imaged Document System.** County may allow OAG to access the County's Imaged Document System to find information on new county child support obligations.
  - iii) **Case Referral Option 3—Paper copies of new child support orders.** County provides paper copies of all new child support obligations to OAG upon the finalization of the orders for support.

If County ever opts to change the referral process, it must provide the OAG at least 30 days notice prior to the proposed change and the OAG must agree to the change. If County ever opts to discontinue the referral process, it must provide the OAG at least 30 days notice prior to the discontinuation.