

TYLER COUNTY COMMISSIONERS COURT
SPECIAL MEETING
JULY 13, 2012

THE STATE OF TEXAS ON THIS THE 13th day of July, 2012 the
Commissioners' Court in and for Tyler County, Texas convened in a Special Meeting at
the Commissioners' Courtroom in Woodville, Texas, the following members of the Court
present, to wit:

JACQUES L. BLANCHETTE	COUNTY JUDGE, Presiding
MARTIN NASH	COMMISSIONER, PCT. #1
RUSTY HUGHES	COMMISSIONER, PCT. #2
MIKE MARSHALL	COMMISSIONER, PCT. #3
JACK WALSTON	COMMISSIONER, PCT. #4
DONECE GREGORY	COUNTY CLERK, EX OFFICIO

The following were absent: none thereby constituting a quorum. In addition to the
above were:

JACKIE SKINNER	COUNTY AUDITOR
SHARON FULLER	COUNTY TREASURER
DAVID HENNIGAN	SHERIFF
AUDREY PELLY	COURT COORDINATOR
JIM ZACHARY	CONSTABLE, PCT. #4
DALE FREEMAN	EMERGENCY MANAGEMENT
KIM NAGYPAL	DISTRICT CLERK
BRYAN WEATHERFORD	JUSTICE OF PEACE, PCT.1/SHERIFF ELECT
JOE SMITH	CRIMINAL DISTRICT ATTORNEY

Commissioner Nash opened the meeting with prayer, and then led in the Pledge of
Allegiance to the Texas Flag.

Terry Riley, Deputy Constable and Courthouse Security Officer presented a Courthouse
Security Standard Operating Procedure.

Commissioner Nash made a motion to approve the minutes from the July 9, 2012
meeting. Commissioner Hughes seconded the motion. All voted yes and none no.

A motion was made by **Commissioner Walston** and seconded by **Commissioner
Marshall** to pay the **Tyler County bills**, as submitted by the County Auditor, which also
includes checks to the fire departments. The county received over \$75,000 from FEMA
to distribute to the fire departments for past "wildfires". There will be subsequent funds
from FEMA according to Mr. Freeman. All voted yes and none no. SEE ATTACHED

Commissioner Marshall motioned to approve the **line item transfers/budget
amendments**, as presented by the **County Auditor**. **Commissioner Walston** seconded
the motion. All voted yes and none no. SEE ATTACHED

Jackie Skinner reported **internet access** for 12 laptop computers in the vehicles of the
Sheriff's department would involve a contract. Sheriff Hennigan stated that Verizon
says it is not a contract because it has no hardware involved and he can cancel it at any
time. The cost will be \$37.99 a month per computer for 12 computers. This will begin
September 1st. A motion was made by **Commissioner Hughes** and seconded by
Commissioner Nash to approve paying for air cards for internet access for the remainder
of 2012 beginning September 1st to December 31st. All voted yes and none no. The cost
of this internet access for next year will be reviewed in budget workshops.

Commissioner Walston made a motion to approve the renewal of the contract with the
Attorney General of Texas Child Support Division for the **State Case Registry/Local
Customer Service** (fiscal year 2013/2014). The motion was seconded by **Commissioner
Marshall**. All voted yes and none no. SEE ATTACHED

A motion was made by **Judge Blanchette** to adopt the **resolution** requesting grant
funding for **software for computers in patrol vehicles**. **Commissioner Walston**
seconded the motion. All voted yes and none no. SEE ATTACHED RESOLUTION

Commissioner Walston motioned to allow the installation of antennae by the **Texas Forest Service** on the County's Doucette tower. The motion was seconded by **Commissioner Nash**. Mr. Freeman stated the Forest Service would pay \$1 per year and agreed to pay for an air conditioner to be installed in the building. All voted yes and none no.

Commissioner Marshall motioned to approve the Communications Site Agreement with the **Texas Forest Service**. **Commissioner Walston** seconded the motion. All voted yes and none no. SEE ATTACHED

No action was taken on bids for the 1997 dump truck and 1995 ½ ton pickup.

Commissioner Hughes made a motion to award the 1999 Dodge pickup and 1997 Aerostar van to Cook and reject bids on the dump truck, army truck and lowboy trailer. **Commissioner Marshall** seconded the motion. All voted yes and none no.

Judge Blanchette motioned to appoint Dr. Sandra Wright to represent Tyler County on the **Regional Steering Committee-1115 Medicaid Waiver/Region 2**. **Commissioner Marshall** seconded the motion. Commissioner Walston stated need to look at putting money for travel in the budget for next year. All voted yes and none no.

Constable Jim Zachary presented the Constables Report. SEE ATTACHED REPORT.

Executive session was not held

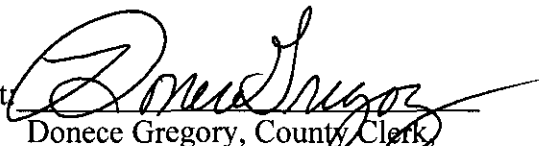
A motion was made by Commissioner Nash to adjourn. Commissioner Marshall seconded the motion. All voted yes.

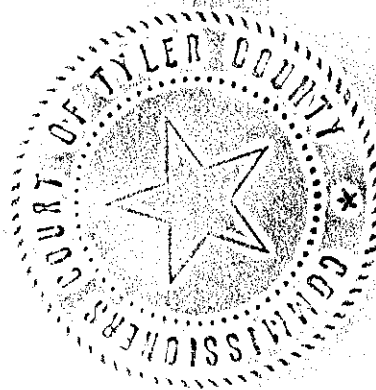
THERE BEING NO FURTHER BUSINESS, THE MEETING ADJOURNED.

I, Donece Gregory, County Clerk and ex officio member of the Tyler County Commissioners Court, do hereby certify to the fact that the above is a true and correct record of the Tyler County Commissioners Court session held on July 13, 2012.

Witness my hand and seal of office on this the 13th day of July, 2012.

Attest


Donece Gregory, County Clerk
Tyler County, Texas



**COURTHOUSE SECURITY
STANDARD OPERATING PROCEDURE**

1.0 Courthouse Security Duties and Responsibilities

1.1 General

1.2 Weapons

1.3 Panic Buttons

1.4 Parking Around Courthouse

1.5 Accidents

1.6 Hallways and Stairways

1.7 Prisoners or Persons in Custody

1.8 Power Outages

1.1 General

Working the security desk in the hallway, you are the ambassador for the county. One of your many jobs is to greet every visitor who walks through the door. Just asking "Can I help you" lets the visitor know that you are aware of your surroundings and you can direct them to where they need to go or answer their questions. Sitting at the desk, watching the cameras, answering questions, directing people, taking care of courthouse operations are just a few of the duties you will face in a day.

1.2 Weapons

- A. Weapons will be referred to as knives, guns, any object with a point or edge.
- B. All weapons will be placed in a clear zip lock bag with two (2) cards with the same number and an identification card for a name and D.L. or I.D. number. One number will be given to the person of the property and the other number will remain in the bag with the weapon. At the end of court, the person may present the number and identification to retrieve the weapon.
- C. If a weapon is not retrieved by the end of the day of court, the weapon will be taken to County Judge's office and the person may retrieve the weapon at that office. If the weapon is not retrieved within thirty (30) days, the weapon becomes property of Tyler County Courthouse System.

1.3 Panic Buttons

When a button has been activated, a piercing, alarm sound will come from that monitor and the screen will show the suite number of where it originated. Proceed to the office where the alarm originated. If everything checks out to be in order there, call dispatch to inform them that there is no need for a deputy. (Note: many times the panic buttons are set off in error, but never "assume" that to be the case. CHECK IT OUT!)

1.4 Parking around the Courthouse

- A. There are three (3) HANDICAP Parking areas. Only vehicles with handicap plates or placards are allowed. All others will be asked to move. If they don't move, call ~~Woodville~~ Police Department to issue a ticket.
Woodville
- B. There is one (1) SHERIFF OFFICE/LAW ENFORCEMENT Parking area at the back of the courthouse. NO OTHER VEHICLES or EMPLOYEES should park there at anytime. If they do, they will be asked to move. All other parking on the street is controlled by the City Police.

1.5 Accident Reports

If ANYONE is injured in or around the courthouse, an accident report MUST be completed by the injured person and any witness that saw the accident. The accident report and/or pictures will need to be given to the County Judge's office and the County D.A.'s office within 72 hours of the accident/incident along with the accident report.

1.6 Hallways and Stairways

These areas must remain clear at all times for fire, safety and the flow of people moving throughout the courthouse. Standing on the stairs or landings is a safety hazard and persons loitering there should be asked to either sit down or step outside the courthouse.

1.7 Prisoners or person in custody.

When a security officer or bailiff is needed to move prisoners or a person put into custody by a judge through the hallways, call the Sheriff's office for transport. NEVER use the elevator unless the prisoner is handicapped.

1.8 Power Outages

The elevator needs to be checked out first. Get a flashlight from the desk and go to the 1st floor elevator door. Knock on the door or call out and if someone answers, assure them that help is on the way. Call "Maintenance Engineering" and inform them about the elevator situation. Have someone stay at the door to keep the person/people informed and to keep them from panicking. Stay in contact with the county Judge's office and Sheriff's Office for updates.

JUDICIAL SERVICES POLICY AND PROCEDURES

2.0 Bailiff Duties and Responsibilities

2.1 Bailiff Responsibilities

2.2 General Courtroom Procedures

2.3 Searches

2.4 Security and Demeanor

2.5 Criminal Documents

2.6 Handling Juries

2.7 Handling Courtroom Evidence

2.8 Holdover Procedures

2.9 Courtroom Arrests

2.10 Fire Emergencies and Evacuations

2.11 Hostage/ Barricaded Person Situations

2.12 Escapes

2.0 Bailiff Duties and Responsibilities

Bailiffs are entrusted to maintain the integrity of the Courts and allow all members of the Court family, Judiciary, litigants, observers and jury members to perform their duties in a safe, protected environment. Rules and Policies may vary from Court to Court but the information attached and present will be at least a minimum standard for Courtroom protocol.

2.1 Bailiff Responsibilities

A. It is the responsibility of the Court Bailiff to become familiar with the procedures and security measure of the court. This will better enable the Bailiff to:

1. Protect the Judiciary
2. Protect members of the Court family
3. Protect all Court participants
4. Protect the integrity of the Jury

2.2 General Courtroom procedures

It is the duty of the bailiff to arrive early enough to prepare the courtroom for the daily business. Some of the general responsibilities are:

- A. Conduct a search of the Courtroom
- B. Conduct a search of the Holding areas
- C. Conduct a search of the Jury Room
- D. Conduct a search of the restrooms attached to the jury room
- E. Search the hallways and public areas in the Courts immediate area
- F. Conduct any responsibilities as per the court

2.3 Searches

Searches of the courtroom and related areas shall be performed at the start of each day that the Courtroom is used. The Bailiff shall insure that no contraband or security violations are present.

Weapons found during your search should be reported immediately to Courthouse Security. Do not touch or move the item in any way and remain in the Courtroom until assistance arrives. Treat this as a Crime Scene and allow no unauthorized persons into the Courtroom until the area is cleared. If you must leave the Courtroom to contact Courthouse Security, clear the Courtroom, lock it, and call for assistance.

Areas to be searched shall include, but are not limited to:

- A. Courtroom Searches
 1. Around all spectator seating
 2. Plaintiffs tables and chairs
 3. Defendants tables and chairs
 4. Jury box and jury chairs
 5. Clerks and Court reporters positions
 6. Judges bench and chair
 7. Witness stand and chair

B. Jury Room Searches

It is important to remove any item or reading material that may contaminate a juror. Weapons or dangerous items should also be considered, as attorneys may use this room for interviews with their client per a Judges order.

1. Check bathrooms under and around toilets
2. Under and on the tables
3. Under and around chairs

2.4 Security and Demeanor during Courtroom proceedings

Anytime a Bailiff feels the need, or even anticipates a need for additional security in the court, the Bailiff should call the Sheriff's office. Security in a courtroom will not be compromised. Priorities of a bailiff are to Protect the Judge and Court staff. Uphold integrity of process. Stay focused on priorities. No clerk duties.

A. Maintaining demeanor is important in any courtroom setting. Each court should have rules as to what is allowed, established by the Judge. The Bailiff will be responsible in the enforcement of the set rules. Establish your presence in the courtroom by commanding authority without arrogance, be neat in your appearance and properly dressed for court.

B. Maintaining security in the courtroom setting is a priority.

1. Officer positioning is utilized to maximize the view of your prisoners, gallery, and staff.
2. Inmate positioning must be maintained to provide maximum security for the Judge and Staff, and to reduce the possibility for escape.
3. At no time shall persons in the gallery be allowed to pass items to an inmate. If a Judge orders any item to be given, the Bailiff will receive the item and ensure it does not contain any contraband.
4. It is the Bailiff's responsibility to inform Courthouse Security of any potential problems that may require additional help.
5. Bailiffs are to keep the head of Courthouse Security informed of any "High Profile" cases anticipated. These trials tend to draw media as well as large numbers of spectators. Additional security may become necessary.

C. Family Courts.

Due to the unknown, **FAMILY COURTS MAY BE THE MOST DANGEROUS AREA IN WHICH TO FUNCTION.** Keep Courthouse Security aware of any arising problems, or potential problems. It is suggested that Bailiffs in your immediate area be made aware of any potential problems.

D. Juvenile Courts

Juvenile Courts are unique as to the handling of Juvenile Prisoners. Bailiffs are to be alert and ready to assist in the event a problem arises. Bailiff's primary duty is to maintain control as to other participants in the courtroom.

2.5 Criminal Dockets

A. Without inmates

1. Review the docket list to see if any of the Defendants have outstanding warrants.
2. When reviewing the criminal history on the County computer, make note of any past charges that could lead to potential problems in the courtroom, i.e.: escape risk, assault, etc.

2.6 Handling Juries

Jurors are an important and integral part of the court system. They shall always be treated with professionalism and dignity.

A. Preparing for a Jury Trial

1. Each Court varies as to the handling of jurors. Check with the Court as to the proper procedures.
2. The Bailiff will position themselves to provide security for the Jury Panel and Court staff during the Voire Dire portion of the trial. Positions will be varied due to staffing and threat level.
3. At the first break, the Bailiff should familiarize the jury with evacuation procedures according to your individual court rules.
4. When the jury is selected, the Bailiff should inquire of any special needs any jury member has, i.e., medical problems.
5. DO NOT discuss anything relative to the proceeding with the jurors. Do not allow any persons to engage in conversation or express an opinion on the proceedings. Words and comments either direct or indirect could result in a mistrial.
6. Bailiffs should be aware of the publicity a trial may produce and guard against news items being read by the jury members that make reference to the trial.
7. Do not give any indication that the sooner the jury reaches a verdict, the sooner they can be released from jury duty.
8. The Bailiff shall be in the immediate area of the Jury room during deliberations unless properly relieved.
9. The Bailiff is not allowed in the Jury room while deliberations are being conducted.
10. If the Judge orders the Bailiff to escort a jury to lunch, Courthouse Security must be notified. No persons will be allowed in the area of the Jury unless authorized by the Judge.

B. Special Jury arrangements requested by the Court.

Sometimes during a trial, or at the conclusion of a trial, a Judge may have special requests for escorting members of the jury from the building. If this does happen, contact Courthouse Security if assistance is needed.

C. Jury misconduct will be immediately reported to the Trial Judge.

D. Sequestered Juries:

1. Primary goals of the Bailiff during a sequestered jury are to provide as much comfort as possible while maintaining the maximum security Level. The Bailiff will attempt to screen the Jury from any incident or information, which may poison the jury.
2. Notify Sheriff's Office and Courthouse Security upon a Jury being sequestered.
3. Insure that any necessary phone numbers are obtained for emergency contacts.
4. If the court conducting a trial in which there is a possibility of sequestering the jury, advise Sheriff's Office and Courthouse Security. It is then important to maintain a flow of information so adequate planning can be done.

E. Illness of a juror

Jurors are the courts responsibility during trial and during times of sequestration. The Bailiff is tasked with the responsibility of rendering and summoning medical aid. Courthouse Security and the Trial Judge will be notified as soon as possible.

2.7 Handling Courtroom Evidence

Although it is the responsibility of the Prosecuting Attorney or person delivering evidence, the Bailiff must be aware of the exhibits offered as evidence. It is advised that the Bailiff contact the attorneys ahead of time as to any possible weapons or other items that may be a potential threat or hazard.

Control of these weapons shall be a priority during the trial, ensuring that the defendant cannot gain access to them.

A. Firearms

1. Firearms shall be checked to insure they are unloaded and/or inoperative.
2. Ammunition shall always be kept separate from firearms, and viewed separately.
3. If firearms are being viewed in the jury room during deliberations, they shall not have access to the ammunition. This evidence must be kept controlled.

B. Dangerous weapons

When viewing knives or other sharp instruments, every precaution will be made for safety.

C. Narcotics

Narcotics should be in a sealed evidence bag. Unless ordered by the Judge, the seal shall never be compromised.

2.8 Holdover Procedures

- A. **IMPORTANT:** Once you enter the Holdover door from the courtroom, you are in the confinement area.
- B. No weapons or ammunition are allowed in the Holdover. (Guns, ASP) OSC Gas will be allowed in the Holdover area for defensive purposes only. If utilized properly, it can be a tremendous asset for inhibiting the ability of inmates attempting to escape.

- C. Holdover keys: The Bailiff must sign out the Holdover key each morning when reporting for duty, and sign them back in at the end of the day. The Bailiff must maintain control of the Holdover key at all times when they are checked out from the Security Office.
- D. Do not leave the key unattended in the door lock. When at lunch or break, lock the key in your office or the gun locker.
- E. Inmates in the Holdovers
1. Male Inmates must be housed separate from Female Inmates.
 2. The number of inmates placed in each Holdover cell shall not exceed the occupancy totals as determined by Jail Standards.
 3. Holdover checks are determined by Jail Standards.
 4. High Risk Inmates shall be housed separate from all other inmates.
 5. Suicidal Inmates must be housed separate from all other inmates. While the inmate is in the cell, a Suicidal Watch sheet shall be established and maintained. You must check on the inmate at least once every thirty minutes unless otherwise noted by confinement directives. It is advised to return them to housing as soon as possible when completed with the Court business.
- G. Bailiff's are not authorized to take urine samples. If a Probation Officer needs a sample, Bailiff's will only stand by for safety purposes, if needed.
- H. Visitation in the Holdovers
1. Family shall not be allowed to visit in the Holdover or Holdover area.
 2. Attorneys will be allowed to visit their clients in the designated area only when the cell door is locked. No physical contact is to be made.
 3. If the Judge orders a contact visit, with an Attorney and an inmate in the holdover, the Bailiff will be positioned where visual contact can be maintained.
 4. Briefcases or other large items are not allowed in the holdover area.
- I. If a Jury is seated in the Jury Box, Bailiffs should not be entering or exiting the holdover area unless directed by the Judge.
- J. Family Courts and Civil Courts
1. These courts do not have holdovers in or adjacent to the courtrooms. Inmates will be seated in the Jury box unless otherwise directed by the court.
 2. Inmates that do not have assault status placed on them, may be seated with leg irons on and the handcuffs removed.

2.9 Courtroom Arrests

Arrests are common in the courtrooms for many different reasons. Each court may have their own preference in the handling of the subjects, but safety shall never be compromised. Depending on the charge, subjects may be handled slightly different while still maintaining the safety and security of the court.

- A. Two primary arrest situations may occur that would be handled differently.

1. Court ordered or a warrant arrest will be handled following the normal court procedure.
 2. Criminal acts personally viewed or done through investigation.
 - a. These arrest will be handled as any normal arrest. Bailiffs will follow the Sheriff's Office protocol as to arrest, reports and evidence.
 - b. Courthouse Security will be notified.
- B. All persons arrested shall be searched prior to placing them in a holdover cell or releasing them to a transport officer. If the arrest is made in a facility not connected to the jail, the prisoner will be handcuffed from behind prior to transport. High Risk prisoners will have leg irons in place as well. Tyler County Sheriff's Office protocol will be followed if Tyler County Sheriff's Office is involved.

2.10 Fire Emergencies and Evacuations

Each Bailiff and Deputy shall be familiar with the Emergency Evacuations Policy.

A. Fire in the Courtroom call 911:

1. Deputies must be aware that it may be a diversion for an escape attempt.
2. Adequate backup should be present prior to any cell doors being opened.
3. Inmates are to be evacuated using the safest route.
4. Areas filled with dense smoke shall not be entered without proper assistance.
4. Courthouse Security should be notified as soon as safely possible.

B. Fire in court areas call 911:

1. Bailiff will immediately secure the prisoners.
2. The area should be cleared of all court personnel.
3. Notify Courthouse Security as soon as possible.

C. Building Evacuation Alarm

County Sheriff's Office is responsible for the safety and security of all persons in county facilities staffed by Judicial Services. This responsibility and authority also includes the courts and related areas. Upon hearing the evacuation alarm, the following procedures are minimum actions that must be done for the safety of all persons.

1. Immediately follow your pre-planned evacuation process (See Section on Emergency Evacuation)
2. DO NOT CALL the Sheriff's Office to check on the authenticity of the alarm. In an evacuation, staff is receiving calls relating to the emergency and re-allocating Deputies for prisoner movement. Once persons within your area of responsibility are in a safe area, report to Courthouse Security.

D. Bomb Threats

Bomb threats are handled on an individual basis. While most are proven to be false, we will act upon all of them. Courthouse Security will determine the need or wisdom of evacuating the building. There may be various reasons not to evacuate, dependent on the information received or the size of the potential explosive. It must be taken into consideration the threat may be an attempt to get a certain person outside.

A bomb threat information form should be placed by all phones. The minimum response will be:

1. Gather all the information possible that was relayed from the caller.
 2. If a specific location was given, clear that area along with any adjoining areas.
 3. Advise the Sheriff's Office and Courthouse Security IMMEDIATELY.
 4. If time allows, conduct a search for any suspicious package.
- ** See Section on Emergency Evacuation

2.11 Hostage/Barricaded Person Situations

The following guidelines should be a minimum response to the incident:

- A. Secure the situation to limit the suspect's movement.
- B. Evacuate persons in the area and adjoining courtrooms.
- C. Advise the Sheriff's Office and Courthouse Security as soon as safely possible. They will assure the Sheriff's Office has been contacted.
- D. UNDER NO CIRCUMSTANCES shall Bailiffs surrender their weapon.

2.12 Escapes

With proper staffing and placement of inmates, this can be kept to a minimum.

- A. Anytime there is an escape from the courtroom the following procedures will be followed:
 1. Immediately advise the Sheriff's Office and other available Security Personnel in the Courtroom, and secure any remaining inmates. Control of any remaining prisoners is essential prior to handling any other matter.
 2. If additional security Personnel are available, they will attempt to apprehend.
 3. If the Court is manned by a single Bailiff:
 - a. If court security will not be compromised, and no other inmates are present in the courtroom, chase may be given.
 - b. If you are the sole Bailiff and no other Security Personnel is assigned, brief other court staff on how they can assist in the event of an escape. Inform them to call the Sheriff's Office with information that needs to be relayed.
 4. Courthouse Security will be advised immediately. If the Panic Button can be activated, do so.
 5. When contacting the Sheriff's Office pass on the following information if it is available.
 - a. Description of the individual. This should include a physical description along with a clothing description.
 - b. The direction of travel, and if accompanied by any other individual(s).
 - c. Advise if Security Personnel are currently giving chase.
 - d. Report any injuries or assistance needed.
 - e. The charge or charges against the individual.
 6. If the subject has family or friends in the courtroom, these persons may need to be detained for investigative purposes.
 7. The Sheriff's Office will conduct the escape investigation and a complete report shall be provided of the incident and charges will be filed.

3.0 Introduction

3.1 Fire

3.2 Severe Weather

3.3 Hazardous Material Spills or Accidents

3.4 Terrorism

3.5 Civil Unrest

3.6 Utility Outages

3.7 Gas Leaks

3.8 Medical Emergencies

3.9 Evacuations

3.10 Vandalism or other damage to Facilities

EMERGENCY EVACUATION PROCEDURES

1. ALL PERSONNEL WILL RETRIEVE PERSONAL BELONGINGS, THAT IS, PURSES, UMBRELLAS, AND COATS.
2. UNDER NO CIRCUMSTANCES WILL ANYONE TURN OFF COMPUTERS, COPIERS, LIGHTS OR MAKE PHONE CALLS, INCLUDING CELL PHONES, DURING THE EVACUATION.
3. ALL PERSONNEL MUST USE THE SAFEST ROUTE TO EXIT THE COURTHOUSE.
4. ALL PERSONNEL WILL GO TO THE HOLDING AREA DESIGNATED AT THE END OF CHARLTON STREET AND WHEAT STREET BEHIND THE COURTHOUSE.
5. A CHECKLIST WILL BE AT THE HOLDING AREA. ALL PERSONNEL MUST CHECK IN FOR ACCOUNTABILITY AND FURTHER INSTRUCTIONS.
6. NO PERSONNEL WILL RETURN TO THE COURTHOUSE UNLESS INSTRUCTED TO DO SO BY THE COUNTY JUDGE OR THE PERSON IN CHARGE. THAT MEANS NO ONE.

3.0 Introduction

The County is exposed to many hazards, all of which have the potential for disrupting County operations, causing damage and creating casualties. The Sheriff's Office is responsible for protecting citizens and employees from the hazards associated with natural disasters and criminal acts, in and around County buildings. Some of the hazards which might affect the County include, but are not limited to: natural disasters such as extreme cold/heat, fires, and severe storms including hurricanes/tornadoes, lightning and hail. Technological disasters include hazardous materials, accidents and power/telephone outages. Other hazards may include bomb threats, vandalism, civil unrest, terrorism and medical emergencies.

The guidelines given below are a plan for emergencies within the Judicial Services.

3.1 Fire

Whether visually witnessed or reported to you, you are considered the First Responder.

A. You should be aware of where the fire extinguishers are located throughout the courthouse.

B. Determine the nature and extent of the fire.

If a small controllable fire is present, (a fire that can be quickly extinguished with little, if any, possibility of it spreading) then put it out using proper fire extinguishers and techniques.

C. Call 9-1-1. Information required for the Fire Department to know is:

1. Where the fire is, to include what floor and which room. Also include some details of the fire if possible.
2. Stay on the phone until the emergency operator releases the line

D. Close all windows and doors in the fire area, if they can be closed without personal risk. Do not lock these doors, as this will hinder the Fire Department in their efforts.

E. Emergency evacuation procedures.

Evacuate the floor, using the stairs, when you are notified there is a fire in the building. **DO NOT CALL TO FIND OUT IF THE ALARM IS REAL TO KEEP FROM EVACUATING.**

1. The last one out of the room should close the door without locking it.
2. Proceed to Emergency exits
3. NEVER use elevators under any circumstances
4. If you have someone in a wheelchair or with a severe medical condition, ask for assistance and/or advice.
5. Stay low to avoid smoke and toxic gases. The best air is close to the floor, so crawl if necessary.
6. If using a stairwell, always proceed to go down unless directed to go up by authorized personnel.
7. Once outside the building, report to your predetermined area and account for persons within your responsibility.

F. Stairways:

It is possible that the Fire Department personnel may be utilizing the stairwells to access the location of the fire. Always stay against the wall when going down a stairwell. If there is smoke, you can guide yourself down by following the wall.

STAY CALM AND ALERT! DO NOT RUN! If a stairwell becomes impassable, cross the floor to another stairwell and continue down. Only proceed to a higher floor if instructed to do so by Fire Department personnel or an authorized person.

If the stairwells are blocked by fire or smoke, return to your office and:

1. Close the door.
2. Call 9-1-1 and give your location.
3. Place towels or clothes, etc. around the doors to prevent smoke from entering.
4. Place a wet towel or cloth over your mouth and nose, then stay low to the floor.
5. Do not break any windows except as a last resort, as this will only provide oxygen for the fire.

G. Do not attempt to re-enter the building until advised by a Fire Department Official or Supervisor. When persons in your area are safely at the predetermined evacuation location, report to your supervisor for further instructions.

3.2 Severe Weather

A. Hurricane/tornado

1. If a hurricane/tornado WATCH has been issued, continue to monitor weather reports. If a hurricane/tornado WARNING is issued for Tyler County and it is in your area, or headed towards your area, take shelter immediately.
2. All personnel must move to the center of the building and slowly progress to the basement. If the basement is full, maintain your position within the center stairwell.
Interior corridors, small interior rooms, basements, interior stairwells are usually safe shelters.
3. Do not use rooms with a large roof expanse. Avoid windows or hallways with doors to the outside at each end. Close all doors to outside rooms.
4. Avoid rooms with large amounts of glass.
5. If the facility is struck, call 9-1-1 for emergency assistance. Check for survivors. Avoid downed power lines, and check for gas leaks and contain small fires.

B. Severe Thunderstorms

Severe thunderstorms may produce high winds, hail and lightning, which may cause damage to county property or facilities.

When a thunderstorm threatens, get inside the building.

3.3 Hazardous Materials Spills or Accidents

Hazardous spills can have a wide reaching impact.

A. It is imperative that all persons and areas be kept up wind of the incident. The following procedures should be followed:

1. Call 9-1-1 to report any release or spill of hazardous materials.
2. Contact your supervisor.

B. In case of imminent danger and emergency response personnel have not yet arrived, the First Responder must decide the appropriate action. If evacuation is ordered, use the evacuation procedures developed for fires. Evacuation in the area of the spill must be

orderly. Persons should go to a secured post and be checked medically, if they have any signs of exposure; breathing difficulties, skin irritation, etc. Persons who have had contact by skin, clothing, shoes, etc. may require de-contamination.

Persons affected or contaminated should be kept separate from unexposed persons to slow the spread of contamination.

C. Crowd control and restricting access to the area may be required. The Fire Department or Emergency Management will give designated safe distance zones. The Fire Department or Emergency Management bears primary responsibility for rescue of personnel and for containment of hazardous materials spills.

D. Call 9-1-1 if a hazardous spill occurs on roadways or railways outside of the facility. They will decide if an evacuation is needed or if it will be best to shelter in place. If the decision is made to shelter in place, close all doors and windows and shut off heating or air conditioning units, which bring in air from outside.

3.4 Terrorism

Terrorism is a highly complex problem and difficult to plan for. All personnel should stay alert to the possibility of terrorism, especially during times of increased international or social tension. Unsecured doors, suspicious persons, or unauthorized vehicles (rental trucks) should be reported to Courthouse Security immediately. When the National Threat Level is rated orange or red, additional security measures will be put into affect.

A. Bomb threats are the form of terrorism that departments will most likely encounter. Experience shows that a majority of all bomb threats are hoaxes, but there is always a chance that a threat may be authentic. The primary rule to remember –**ALL BOMB THREATS ARE REAL**– With any bomb threat, standard procedures should be followed at all times to provide for the safety of employees, the public and property.

1. If the threat is by telephone, try to get all the information possible on the person or group making the threat and the size, type and location of the bomb. A bomb threat questionnaire kept near telephones and used to gather necessary information may be the single most important resource in dealing with bomb threats. Don't hesitate to ask for their name and address; it is a possibility that a caller will give this information to you.
2. Do not become excited or display emotion.
3. Pay close attention to detail and listen for background noises.
4. Upon termination of the call, notify a Supervisor immediately. **SUSPEND RADIO /CELL PHONE USAGE.** (Reminder: Some radio transmissions in close proximity may cause premature detonation of blasting caps or electronic detonation devices.) Supervisors will notify necessary emergency personnel. Utilize person-to-person communications.
5. No evacuation of the building will be conducted unless instructed to do so.
6. Search teams may be established and deployed by the on-scene supervisor. Employees familiar with the area may be asked to search for unfamiliar briefcases, packages, bags, boxes, or other objects. Do not touch or attempt to move any object that appears suspicious. If a suspicious object is found, evacuate the immediate area and advise supervision.

B. Establishing a perimeter

1. An outside perimeter should be established for pedestrian traffic safety, if an

evacuation has been ordered. No civilians or employees that are outside at the time will be allowed entry/re-entry into the building, until it is declared safe, and then only after office staff has been allowed to enter in order to secure their respective offices.

2. Security personnel shall exercise close observation of surrounding buildings, vehicles and pedestrian traffic for suspicious activity.

C. Personnel/Judges/high profile case witnesses/victims who have recently received terroristic threats should be provided with a special escort and expeditiously evacuated to a protected area.

D. All Security/Bailiff personnel will be readily available to assume duties as assigned by the on-scene supervisor until relieved, or authorized to return to your normal duty assignment.

E. If evacuation is required, advise the Sheriff's Office of inmates or prisoners to be moved.

3.5 Civil Unrest

During periods of increased tensions, employees should be alert to the possibility of civil unrest. Anyone outside or around any county building protesting should be reported to Courthouse Security. Protesting is not against the law, but can lead to a large crowd. A large group of protestors wanting media attention may turn to unlawful acts to gain that attention. Security must be made aware of the situation to plan for additional personnel.

3.6 Utility Outages

A. In the case of an electrical outage, turn off equipment that draws a large amount of current. Turn off computers to prevent damage from a power surge.

B. Keep flashlights and spare batteries available. If none are available, contact your supervisor.

3.7 Gas Leaks

Natural gas leaks bring the danger of an explosion.

A. If a gas odor is detected in the building:

1. Contact Courthouse Security
2. An authorized person will determine if an evacuation is necessary. Follow your evacuation procedures. Evacuate to a safe distance from the building.
3. Do not re-enter the building until the Fire Department or authorized personnel has declared the building safe.

3.8 Medical Emergencies

As a certified Peace Officer you have certain responsibilities and obligations. It is your duty to render aid to ANY injured person.

A. Serious illness or injury of an employee or member of the public, call 9-1-1- and give the following information:

1. Self-identification
2. Location and address
3. Location of patient and approximate age
4. Type of injury or symptoms of illness, if known.
5. If more than one victim, the number affected.

B. If the situation requires use of an AED, proceed. You do not need certificated to use an AED.

C. Medical emergency involving inmates.

1. If not life threatening, contact the Sheriff's Office. They will determine what needs to be done.
2. If life threatening, call 9-1-1.

D. Courthouse Security will meet medical responders at the door and direct them to the scene.

E. If the injury is the result of criminal activity or potential negligence, assign a different person to isolate and keep witnesses separated.

3.9 Evacuations

Evacuations will be required from time to time in county buildings. Bailiffs and Courthouse Security Officers will be responsible for safe and orderly evacuations.

A. **STAY CALM AT ALL TIMES.** Your demeanor in an emergency sets the stage for everyone around you.

B. Employees and citizens will exit the building by the predetermined Fire/Safety written plan.

C. Bailiffs should check the floor they are on for the persons that have NOT evacuated or are Physically Challenged Persons.

D. Persons refusing to evacuate, and persons requiring assistance in evacuation should be reported to Courthouse Security. The Security Desk can relay your information by radio.

E. Bailiff/Security Officers should be familiar with all stairwells and exit points of the building. You may be required to assist persons trapped in a stairwell due to an impairment.

F. In the event of a fire, evacuated persons should be far enough away to ensure that no one impedes Emergency personnel or will be injured from falling debris.

G. If an evacuation is ordered for a bomb threat or gas leak, persons should note where the Fire Department has staged. Persons should evacuate behind the Fire Department.

H. Bailiffs/Security Officers may be asked to assist in traffic control. This is to expedite persons crossing city streets and getting them clear of a threat area. When persons are

safely away from the building, Bailiffs /Security Officers will return to authorized personnel for further instruction.

I. Inmates or prisoners inside of the building must be evacuated. The Sheriff's Office will be charged with the responsibility of inmate movement.

J. If in the Judicial Center, inmates will be evacuated through the secured hallways.

K. Inmates in the custody of the Tyler County Sheriff's Office will be handled per Tyler County Sheriff's Office protocol.

L. If inmates are in the Family Courts, Courthouse or Juvenile Courts, you will ensure that restraints are in place. Inmates will then be escorted to the closest exit. Transportation drivers will meet you and secure the inmates or prisoners in the unit and return them back to jail.

3.10 Vandalism or other damage to County Facilities or Property

A. Report the incident to Courthouse Security. Crime scene may be required, and an Officer will make the report.

B. The Engineer Department will be notified for repair of damage. If the damage takes place after hours and requires emergency repairs to secure the facility, contact your supervisor. Officers may be required to remain at the facility until broken windows or doors which may compromise the facility's security are repaired.

EMERGENCY PROCEDURES

Courthouse Security/Bailiffs Duties & Responsibilities

BAILIFF POLICIES AND PROCEDURES

4.0 Bailiff Duties and Responsibilities

4.1 Bailiff Responsibilities

4.2 General Courtroom Procedures

4.3 Searches

4.4 Security and Demeanor During Courtroom Proceedings

4.5 Criminal Dockets

4.6 Handling Juries

4.7 Handling Courtroom Evidence

4.8 Bailiff Procedures

4.0 Bailiff Duties and Responsibilities

Bailiffs are entrusted to maintain the integrity of the Courts and allow all member of the Court family, Judiciary, and jury members to perform their duties in a safe protected environment. Rules and Policies may vary from Court to Court but the information attached and present will be at least a minimum standard for Courtroom protocol.

4.1 Bailiff Responsibilities

A. It is the responsibility of the Court Bailiff to become familiar with the procedures and security measure of the court. This will better enable the Bailiff in to:

1. Protect the Judiciary
2. Protect members of the Court family
3. Protect all Court participants
4. Protect the integrity of the Jury

4.2 General Courtroom procedures

It is the duty of the bailiff to arrive early enough to prepare the courtroom for the daily business. Some of the general responsibilities are:

- A. Conduct a search of the Courtroom
- B. Conduct a search of the Holding areas
- C. Conduct a search of the Jury Room
- D. Conduct a search of the restrooms attached to the jury room
- E. Search the hallways and public areas in the Courts immediate area
- F. Conduct any responsibilities as per the court

4.3 Searches

Searches of the courtroom and related areas shall be performed at the start of each day that the Courtroom is used. The Bailiff shall insure that no contraband or security violations are present.

Weapons found during your search should be reported immediately to courthouse security. Do not touch or move the item in any way and remain in the Courtroom until assistance arrives. Treat this as a Crime Scene and allow no unauthorized persons into the Courtroom until the area is cleared. If you must leave the Courtroom to contact courthouse security, clear the Courtroom, lock it, and call for assistance.

Areas to be searched shall include, but are not limited to:

A. Courtroom Searches

1. around all spectators seating
2. Plaintiffs tables and chairs
3. Defendants tables and chairs
4. Jury box and jury chairs
5. Clerks and Court reporters positions
6. Judges bench and chair
7. Witness stand and chair

B. Jury Room Searches

It is important to remove any item or reading material that may contaminate a juror. Weapons or dangerous items should also be considered, as attorneys may use this room for interviews with their client per a Judge's order.

1. Check bathrooms under and around toilets
2. Under and on the tables
3. Under and around chairs

4.4 Security and Demeanor during Courtroom proceedings

Anytime a Bailiff feels the need, or even anticipates a need for additional security in the court, call the Sheriff's office for assistance. Security in a courtroom will not be compromised.

A. Maintaining demeanor is important in any courtroom setting. Each court should have rules as to what is allowed, established by the Judge. The Bailiff will be responsible in the enforcement of the set rules.

B. Maintaining security in the courtroom setting is a priority.

1. Officer positioning is utilized to maximize the view of your prisoners, gallery, and staff.
2. Inmate positioning must be maintained to provide maximum security for the Judge and Staff, and to reduce the possibility for escape.
3. At no time shall persons in the gallery be allowed to pass items to an inmate. If a Judge orders any item to be given, the Bailiff will receive the item and ensure it does not contain any contraband.
4. It is the Bailiff's responsibility to inform supervision of any potential problems that may require additional help.
5. Bailiffs are to keep the head of Courthouse Security informed of any High Profile cases anticipated. These trials tend to draw media as well as large numbers of spectators. Additional security may become necessary.

C. Family Courts.

Due to the unknown, Family Courts may be the most dangerous area in which to function. Keep Courthouse Security aware of any arising problems, or potential problems. It is suggested that Bailiffs in your immediate area be made

aware of any potential problems.

D. Juvenile Courts

Juvenile Courts are unique as to the handling of Juvenile Prisoners. Probation Officers handle the movement of prisoners in these courts. Bailiffs are to be alert and ready to assist in the event a problem arises. Bailiff=s primary duty is to maintain control as to other participants in the courtroom.

4.5 Criminal Dockets

A. Without inmates

1. Review the docket list to confirm Defendants are not in custody. If they are in custody, you will need to order the inmate and bring them to Court.
2. Review the docket list to see if any of the Defendants have outstanding warrants on the County Computer, not TCIC or NCIC.
3. When reviewing the criminal history on the County computer, make note of any past charges that could lead to potential problems in the courtroom, i.e.: escape risk, assault, etc.

B. With inmates

4.6 Handling Juries

Jurors are an important and integral part of the court system. They shall always be treated with professionalism and dignity.

A. Preparing for a Jury Trial

1. Each Court varies as to the handling of jurors. Check with the Court as to the proper procedures.
2. The Bailiff will position themselves to provide security for the Jury Panel and

Court staff during the Voire Dire state of the trial. Positions will be varied due to staffing and threat level.

3. At the first break, the Bailiff should familiarize the jury with evacuation procedures according to your individual court rules.
4. When the jury is selected, the Bailiff should inquire of any special needs any jury member has, i.e.: medical problems.
5. DO NOT discuss anything relative to the proceeding with the jurors. Do not allow any persons to engage in conversation or express an opinion on the proceedings. Words and comments either direct or indirect could result in a mistrial.
6. Bailiffs should be aware of the publicity a trial may produce and guard against news items being read by the jury members that make reference to the trial.
7. Do not give any indication that the sooner the jury reaches a verdict, the sooner they can be released from jury duty.
8. The Bailiff shall be in the immediate area of the Jury room during deliberations unless properly relieved.
9. The Bailiff is not allowed in the Jury room while deliberations are being conducted.
10. If the Judge orders the Bailiff to escort a jury to lunch, Courthouse Security must be notified. No persons will be allowed in the area of the Jury unless authorized by the Judge.

B. Special Jury arrangements requested by the Court.

Sometimes during a trial, or at the conclusion of a trial, a Judge may have special requests for escorting members of the jury from the building. If this does happen, contact Courthouse Security if assistance is needed.

C. Jury misconduct will be immediately reported to the Trial Judge.

D. Sequestered Juries:

1. Primary goals of the Bailiff during a sequestered jury are to provide as much comfort as possible while maintaining the maximum security Level. The Bailiff will attempt to screen the Jury from any incident or information, which may poison the jury.
2. Notify Courthouse Security upon a Jury being sequestered.
3. Insure that any necessary phone numbers are obtained for emergency contacts.
4. If the court conducting a trial in which there is a possibility of sequestering the jury, advise Courthouse Security. It is then important to maintain a flow of information so adequate planning can be done.

E. Illness of a juror

Jurors are the courts responsibility during trial and during times of sequestration. The Bailiff is tasked with the responsibility of rendering and summoning medical aid. Courthouse Security and the Trial Judge will be notified as soon as possible.

4.7 Handling Courtroom Evidence

The Bailiff must be aware of the exhibits offered as evidence. It is advised that the Bailiff contact the attorneys ahead of time as to any possible weapons or other items that may be a potential threat or hazard.

Control of these weapons shall be a priority during the trial, ensuring that the defendant cannot gain access to them.

A. Firearms

1. Firearms shall be checked to insure they are unloaded and/or inoperative.
2. Ammunition shall always be kept separate from firearms, and viewed separately.

3. If firearms are being viewed in the jury room during deliberations, they shall not have access to the ammunition. This evidence must be kept controlled.

B. Dangerous weapons

When viewing knives or other sharp instruments, every precaution will be made for safety.

C. Narcotics

Narcotics should be in a sealed evidence bag. Unless ordered by the Judge, the seal shall never be compromised.

4.8 Bailiff Procedures

A. Bailiff's are not authorized to take urine samples. If a Probation Officer needs a sample, Bailiff's will only stand by for safety purposes, if needed.

B. Visitation During Court

1. Family shall not be allowed to visit in courtroom or jury room.
2. Attorneys will be allowed to visit in the jury room only when the door is locked.
No physical contact is to be made.
3. If the Judge orders a contact visit, with an Attorney and an inmate in the jury room, the Bailiff will be positioned where visual contact can be maintained.
4. Briefcases or other large items are not allowed into the jury room.

I. If a Jury is seated in the Jury Box, Bailiffs should not be entering or exiting the jury room area unless directed by the Judge.

J. Family Courts and Civil Courts

1. These courts do not have holdovers in or adjacent to the courtrooms.

Inmates will be seated in the Jury box unless otherwise directed by the court.

2. Inmates that do not have assault status placed on them may be seated with leg irons on and the handcuffs removed.



Tyler County

Accounts Payable

July 13, 2012



Tyler County, TX

CHECK REGISTER

By Fund

Payable Dates 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Fund: 010 - GENERAL FUND							
Tyler County Booster	105276	07/13/2012	NOTICE EARLY VOTING/COCL	010-401-42158		07/13/2012	94.80
Tyler County Booster	105276	07/13/2012	EARLY VOTING/COCLK	010-401-42158		07/13/2012	94.80
Tyler County Booster	105276	07/13/2012	INV.#0027556/ADVERTISING	010-401-42616		07/13/2012	72.00
Tyler County Booster	105276	07/13/2012	INV.#0027667/DSCLK	010-407-42100		07/13/2012	690.14
Lakeway Tire & Service-Jasp	105212	07/13/2012	1063/TCSO	010-426-42400		07/13/2012	41.00
Lakeway Tire & Service-Jasp	105212	07/13/2012	1063/TCSO	010-426-42401		07/13/2012	12.00
Sirchie Fingerprint Laborator	105254	07/13/2012	00-A75979/TCSO	010-426-42182		07/13/2012	63.11
Tyler Technologies, Inc.	105280	07/13/2012	41637/COAUD	010-401-42178		07/13/2012	3,130.35
Legal Directories Publishing	105215	07/13/2012	C430349/COCLK	010-402-42100		07/13/2012	14.50
Stamps Office Supply "The C	105257	07/13/2012	INV.#065579/TCSO	010-426-42100		07/13/2012	539.44
Stamps Office Supply "The C	105257	07/13/2012	INV.#065810/TCSO	010-426-42100		07/13/2012	533.41
Mann, Robert H. ATTY.	105218	07/13/2012	JACOBS, ANGEL	010-415-42634		07/13/2012	1,125.00
Mann, Robert H. ATTY.	105218	07/13/2012	POKORNEY, STEPHEN WAYN	010-415-42634		07/13/2012	1,125.00
TDCA/Texas District Court All	105262	07/13/2012	REGIS./NAGYPAL, KIM	010-407-42659		07/13/2012	30.00
Mann, Robert H. ATTY.	105218	07/13/2012	POKORNEY, STEPHEN WAYN	010-415-42634		07/13/2012	225.00
Sampson, Douglas	105249	07/13/2012	INV.#12-01050/COJUD	010-442-42412		07/13/2012	505.00
U S Flag & Flagpole Supply, L	105282	07/13/2012	INV.#12-1741/COJUD	010-442-42412		07/13/2012	144.00
Cypher Technologies	105167	07/13/2012	INV.#1227/COMMISSIONERS	010-440-42353		07/13/2012	120.00
Cypher Technologies	105167	07/13/2012	INV.#1228/COMMISSIONERS	010-440-42353		07/13/2012	60.00
Cypher Technologies	105167	07/13/2012	INV.#1229/EXT.	010-440-42353		07/13/2012	60.00
Cypher Technologies	105167	07/13/2012	INV.#1230/EOC	010-440-42353		07/13/2012	60.00
Radiology Associate LLP	105246	07/13/2012	GRIFFITH, RICHARD E./TCSO	010-401-42667		07/13/2012	506.00
Radiology Associate LLP	105246	07/13/2012	GRIFFITH, RICHARD E./TCSO	010-401-42667		07/13/2012	76.00
Walling Signs & Graphics/Pa	105289	07/13/2012	INV.#13341/COJUD	010-442-42412		07/13/2012	150.00
Advanced Systems & Alarms	105144	07/13/2012	INV.#136209	010-442-42412		07/13/2012	111.00
Walling Signs & Graphics/Pa	105289	07/13/2012	INV.#13997/COCLK	010-402-42100		07/13/2012	57.95
Belt Harris Pechacek, LLLP	105152	07/13/2012	INV.#15645/COJUD	010-401-42668		07/13/2012	7,500.00
Belt Harris Pechacek, LLLP	105152	07/13/2012	INV.#15652/COAUD	010-401-42668		07/13/2012	15,150.00
Innovative Office Systems	105204	07/13/2012	TYLCOT/TAX	010-401-42111		07/13/2012	419.93
Innovative Office Systems	105204	07/13/2012	TYLCOUCLE/COCLK	010-440-42101		07/13/2012	74.93
CMA Communications	105160	07/13/2012	163030408/TCSO	010-427-42108		07/13/2012	103.08
Oce' Financial Services Inc.	105233	07/13/2012	200-5028484-000/COAUD	010-440-42677		07/13/2012	218.00
Story-Wright	105259	07/13/2012	104307/COAUD	010-440-42101		07/13/2012	16.78
Story-Wright	105259	07/13/2012	104307/COAUD	010-440-42101		07/13/2012	5.79
Story-Wright	105259	07/13/2012	104307/COAUD	010-422-42100		07/13/2012	11.99
Story-Wright	105259	07/13/2012	104307/COAUD	010-440-42101		07/13/2012	151.91
Staples Credit Plan	105258	07/13/2012	6035517820773694/PRECIN	010-453-43210		07/13/2012	1,279.93

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Indoff Office Supplies	105202	07/13/2012	183748/COJUD	010-440-42101		07/13/2012	50.96
Indoff Office Supplies	105202	07/13/2012	187474/DSCLK	010-407-42100		07/13/2012	44.46
Indoff Office Supplies	105202	07/13/2012	083749/TREAS.	010-423-42100		07/13/2012	201.86
Indoff Office Supplies	105202	07/13/2012	186597/VET. SRV.	010-405-42100		07/13/2012	127.99
Indoff Office Supplies	105202	07/13/2012	186597/VET. SRV.	010-405-42100		07/13/2012	220.94
Meek, Donald	105221	07/13/2012	OVERPYMT/CS#T85121	010-401-48000		07/13/2012	108.00
Gavino, Ramos	105191	07/13/2012	OVERPYMT./CS#T85328	010-401-48000		07/13/2012	50.00
Wheat, Josiah Jr.	105294	07/13/2012	3RD QTR. LEASE/WHEAT BLD	010-442-42220		07/13/2012	250.00
Seale, Elizabeth Wheat	105251	07/13/2012	3RD QTR. LEASE/WHEAT BLD	010-442-42220		07/13/2012	250.00
Zeavin, Jennifer Wheat	105302	07/13/2012	3RD QTR. LEASE/WHEAT BLD	010-442-42220		07/13/2012	250.00
Roberts, Julia Wheat	105247	07/13/2012	3RD QTR. LEASE/WHEAT BLD	010-442-42220		07/13/2012	250.00
CIT	105159	07/13/2012	930-0039477-000/JP. 1	010-440-42677		07/13/2012	85.30
Nagypal, Kim / District Clerk	105228	07/13/2012	GRAND JURY/JUNE 2012 TER	010-408-42689		07/13/2012	80.00
DP Solutions, Inc.	105177	07/13/2012	INV.#246171/COCLK	010-440-42101		07/13/2012	129.00
DP Solutions, Inc.	105177	07/13/2012	INV.#246350/COCLK	010-440-42353		07/13/2012	243.00
DP Solutions, Inc.	105177	07/13/2012	INV.#246581/COCLK	010-440-42353		07/13/2012	287.85
Oce' Imagistics Inc.	105234	07/13/2012	SR4199/COADU	010-440-42101		07/13/2012	38.00
Texas Association of Countie	105264	07/13/2012	2ND QTR. 2012	010-401-40140		07/13/2012	1,395.02
Elliott Electric Supply, Inc.	105182	07/13/2012	3223109/COJUD	010-442-42412		07/13/2012	228.00
Service by Scott	105252	07/13/2012	INV.#3630/COJUD	010-442-42412		07/13/2012	271.06
Sparkletts & Sierra Springs	105255	07/13/2012	21549393631084/TAX	010-440-42101		07/13/2012	32.87
Sparkletts & Sierra Springs	105255	07/13/2012	21549393631084/TAX	010-440-42101		07/13/2012	28.19
Service by Scott	105252	07/13/2012	INV.#3642/TCSO	010-442-42411		07/13/2012	213.57
Quill Corporation	105245	07/13/2012	C3420103/COCLK	010-402-42100		07/13/2012	148.47
LEAF	105214	07/13/2012	100-1360627-001/COAUD	010-440-42677		07/13/2012	79.61
Tolars Feed & Outdoor Suppl	105269	07/13/2012	STMT. #14370/TCSO	010-426-42656		07/13/2012	44.85
Tolars Feed & Outdoor Suppl	105269	07/13/2012	STMT.#14370/TCSO	010-426-42656		07/13/2012	13.90
Quill Corporation	105245	07/13/2012	C3338775/EXT.	010-439-42100		07/13/2012	63.51
Tolars Feed & Outdoor Suppl	105269	07/13/2012	STMT.#14370/TCSO	010-426-42656		07/13/2012	17.95
Tolars Feed & Outdoor Suppl	105269	07/13/2012	STMT. #14370/TCSO	010-426-42656		07/13/2012	19.90
Tolars Feed & Outdoor Suppl	105269	07/13/2012	STMT.#14370/TCSO	010-426-42656		07/13/2012	19.90
Quill Corporation	105245	07/13/2012	C3338775/EXT.	010-439-42100		07/13/2012	2.49
East Texas Support Services,	105179	07/13/2012	3RD. QTR/NUTR. CTR.	010-401-42352		07/13/2012	3,750.00
Wilson Insurance Agency	105298	07/13/2012	NOTARY BOND/FORD, LISA	010-427-42900		07/13/2012	71.00
Tyler County Hospital	105277	07/13/2012	PELLERT, RONALD A./TCSO	010-401-42667		07/13/2012	240.00
Parker Lumber - Woodville	105237	07/13/2012	22760/TCSO	010-442-42511		07/13/2012	219.03
Tyler County Hospital	105277	07/13/2012	LEJUNE, DANA/COCLK	010-401-48000		07/13/2012	42.00
A T & T / Phone Lines / Carol	105140	07/13/2012	ELEVATOR	010-442-42422		07/13/2012	81.03
A T & T / Phone Lines / Carol	105140	07/13/2012	COUNTY CLERK	010-402-42500		07/13/2012	186.91
A T & T / Phone Lines / Carol	105140	07/13/2012	DISTRICT JUDGE	010-409-42500		07/13/2012	27.54
A T & T / Phone Lines / Carol	105140	07/13/2012	EXTENSION OFFICE	010-439-42500		07/13/2012	55.08
A T & T / Phone Lines / Carol	105140	07/13/2012	COMMISSIONERS COURT	010-401-42519		07/13/2012	218.34
A T & T / Phone Lines / Carol	105140	07/13/2012	TREASURER	010-423-42500		07/13/2012	27.54
A T & T / Phone Lines / Carol	105140	07/13/2012	DISTRICT CLERK	010-407-42500		07/13/2012	57.23

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
A T & T / Phone Lines / Carol	105140	07/13/2012	VETERANS SRV.	010-405-42500		07/13/2012	157.76
A T & T / Phone Lines / Carol	105140	07/13/2012	DATA PROCESSING	010-440-42350		07/13/2012	161.61
A T & T / Phone Lines / Carol	105140	07/13/2012	JP. 1	010-411-42500		07/13/2012	85.92
A T & T / Phone Lines / Carol	105140	07/13/2012	TCSO	010-426-42500		07/13/2012	699.26
A T & T / Phone Lines / Carol	105140	07/13/2012	COUNTY AUDITOR	010-422-42500		07/13/2012	55.08
A T & T / Phone Lines / Carol	105140	07/13/2012	COUNTY JUDGE	010-421-42500		07/13/2012	140.41
A T & T / Phone Lines / Carol	105140	07/13/2012	TAX OFFICE	010-420-42500		07/13/2012	287.13
A T & T / Phone Lines / Carol	105140	07/13/2012	PARKS/WILDLIFE	010-430-42502		07/13/2012	27.54
A T & T / Phone Lines / Carol	105140	07/13/2012	DPS	010-430-42500		07/13/2012	108.57
A T & T / Phone Lines / Carol	105140	07/13/2012	DRIVERS LICENSEW	010-430-42503		07/13/2012	55.08
A T & T / Phone Lines / Carol	105140	07/13/2012	DISTRICT ATTY.	010-419-42500		07/13/2012	192.78
West Bluff Emerg Physicians	105292	07/13/2012	CHAPMAN, WALTER/DVIO05	010-401-42667		07/13/2012	1,240.00
Larry Trest Auto Brokers, Inc.	105213	07/13/2012	5-30-12/TCSO	010-426-42413		07/13/2012	251.33
Larry Trest Auto Brokers, Inc.	105213	07/13/2012	5-31-12/TCSO	010-426-42413		07/13/2012	373.53
Tyler County Hospital	105277	07/13/2012	PHELPS, RICHARD/COJUD	010-401-48000		07/13/2012	42.00
Key Equipment Finance	105210	07/13/2012	5911122861/TAX	010-440-42677		07/13/2012	75.07
Larry Trest Auto Brokers, Inc.	105213	07/13/2012	6-12-12/TCSO	010-426-42413		07/13/2012	130.10
Larry Trest Auto Brokers, Inc.	105213	07/13/2012	6-21-12/TCSO	010-426-42413		07/13/2012	249.50
T. Bell Services	105261	07/13/2012	6-22-12/TCSO	010-442-42511		07/13/2012	81.50
Gregory, Donece	105193	07/13/2012	MILEAGE/CO. CLK. CONFERN	010-402-42659		07/13/2012	152.07
Jarrots Pharmacy	105207	07/13/2012	BAREFIELD, REGINALD/TCSO	010-401-42667		07/13/2012	26.13
Jarrots Pharmacy	105207	07/13/2012	CHAPMAN, WALTER/TCSO	010-401-42667		07/13/2012	147.15
Jarrots Pharmacy	105207	07/13/2012	DIANNI, ARMON/TCSO	010-401-42667		07/13/2012	46.26
Jarrots Pharmacy	105207	07/13/2012	KELLY, CHRISTOPHER/TCSO	010-401-42667		07/13/2012	68.92
Jarrots Pharmacy	105207	07/13/2012	LEWIS, JOSEPH/TCSO	010-401-42667		07/13/2012	588.07
Jarrots Pharmacy	105207	07/13/2012	MADDOX, JOSHUA/TCSO	010-401-42667		07/13/2012	23.86
Jarrots Pharmacy	105207	07/13/2012	MUNDAY, KENNETH/TCSO	010-401-42667		07/13/2012	7.99
Jarrots Pharmacy	105207	07/13/2012	PELLERT, RONALD/TCSO	010-401-42667		07/13/2012	123.71
Jarrots Pharmacy	105207	07/13/2012	TYLER COUNTY/TCSO	010-401-42667		07/13/2012	3.29
Jarrots Pharmacy	105207	07/13/2012	THOMAS, SHAWN P./TCSO	010-401-42667		07/13/2012	16.18
Jarrots Pharmacy	105207	07/13/2012	WIGGINS, ELVIS/TCSO	010-401-42667		07/13/2012	145.05
Timberman's Supply	105268	07/13/2012	247144/TCSO	010-442-42511		07/13/2012	20.59
Parker Lumber - Woodville	105237	07/13/2012	22710/JUST. CTR.	010-442-42411		07/13/2012	342.88
Parker Lumber - Woodville	105237	07/13/2012	22725/COURTHOUSE	010-442-42412		07/13/2012	431.71
Sullivan's Hardware	105260	07/13/2012	JUNE 2012/TCSO	010-442-42411		07/13/2012	3.99
Wilson Insurance Agency	105298	07/13/2012	NOTARY	010-427-42900		07/13/2012	71.00
Woodville Veterinary Clinic	105300	07/13/2012	265/TCSO	010-426-42656		07/13/2012	87.40
Tyler County Hospital	105277	07/13/2012	KELLEY, CHRISTOPHER/TCSO	010-401-42667		07/13/2012	763.72
Entergy	105184	07/13/2012	2977369/WHEAT BLDG.	010-442-42512		07/13/2012	301.68
Entergy	105184	07/13/2012	3468292/BEST BLDG.	010-442-42516		07/13/2012	599.74
Entergy	105184	07/13/2012	521353/TCSO	010-442-42511		07/13/2012	99.25
Entergy	105184	07/13/2012	521552/COURTHOUSE	010-442-42515		07/13/2012	1,573.57
Entergy	105184	07/13/2012	521577/JUST. CTR.	010-442-42511		07/13/2012	3,279.30
Entergy	105184	07/13/2012	619032/TAX	010-442-42517		07/13/2012	524.00

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
WalMart Community/GECRB	105290	07/13/2012	6899/COCLK	010-401-42158		07/13/2012	12.27
Music Mountain Water Com	105225	07/13/2012	82270201/COCLK	010-440-42101		07/13/2012	32.24
Modica Bros.	105222	07/13/2012	JUNE 2012/COJUD	010-442-42412		07/13/2012	8.00
Modica Bros.	105222	07/13/2012	JUNE 2012/TCSO	010-426-42400		07/13/2012	264.20
Modica Bros.	105222	07/13/2012	JUNE 2012/TCSO	010-426-42401		07/13/2012	1,622.35
Modica Bros.	105222	07/13/2012	JUNE 2012/TCSO	010-426-42413		07/13/2012	571.39
Direct Solutions	105174	07/13/2012	INV.#6379-1/COJUD	010-442-42106		07/13/2012	56.83
Direct Solutions	105174	07/13/2012	INV.#6570/COJUD	010-442-42106		07/13/2012	421.79
Direct Solutions	105174	07/13/2012	INV.#6615/COAUD	010-440-42101		07/13/2012	589.95
Texas Imaging Systems, Inc. (105265	07/13/2012	001-0097404-001/TCSO	010-440-42677		07/13/2012	188.40
Innovative Leasing	105203	07/13/2012	001-0034127-002/TAX	010-440-42677		07/13/2012	867.99
Verizon Wireless	105286	07/13/2012	6855-00001/TCSO	010-426-42500		07/13/2012	1,342.47
Verizon Wireless	105285	07/13/2012	8019-00001/COJUD	010-442-42412		07/13/2012	127.95
Verizon Wireless	105287	07/13/2012	5066-00001/PHONE	010-411-42500		07/13/2012	74.91
Hennigan, David	105197	07/13/2012	PER DIEM/HIDTA TRAINING	010-426-42659		07/13/2012	250.00
Powers, Carol	105243	07/13/2012	PER DIEM/CRT. CLK. CONFER	010-411-42661		07/13/2012	200.00
Turner, Tina	105273	07/13/2012	PER DIEM/CRT. CLK SEMINA	010-411-42661		07/13/2012	200.00
Hilton Bella Harbor	105198	07/13/2012	REGIS./POWERS, CAROL L.	010-411-42661		07/13/2012	237.30
Hilton Bella Harbor	105199	07/13/2012	REGIS./TURNER, TINA	010-411-42661		07/13/2012	237.30
Byron, Stefani	105156	07/13/2012	PER DIEM/SAF VIC CONFERE	010-426-42659		07/13/2012	171.00
Tyler County Hospital	105277	07/13/2012	CARRUTH, MICHAEL R./TCSO	010-401-48000		07/13/2012	42.00
Pelly Electronics	105239	07/13/2012	INV.#720/EXT.	010-440-42353		07/13/2012	240.00
Telstar Specialty Products	105263	07/13/2012	INV.#7242/TCSO	010-427-42108		07/13/2012	843.35
Telstar Specialty Products	105263	07/13/2012	INV.#7330/TCSO	010-427-42108		07/13/2012	324.65
Telstar Specialty Products	105263	07/13/2012	INV.#7363/TCSO	010-427-42108		07/13/2012	1,215.65
Telstar Specialty Products	105263	07/13/2012	INV.#7392	010-427-42108		07/13/2012	381.90
Telstar Specialty Products	105263	07/13/2012	INV.#7393/TCSO	010-427-42108		07/13/2012	82.90
FedEx	105185	07/13/2012	2212-3061-2/COAUD	010-401-42111		07/13/2012	94.12
FedEx	105185	07/13/2012	1706-0613-2/TCSO	010-401-42111		07/13/2012	24.73
U Pump It - Gardner Oil	105281	07/13/2012	UP TYCO COURTHOUSE/COJ	010-442-42412		07/13/2012	224.12
U Pump It - Gardner Oil	105281	07/13/2012	UP TYCO COURTHOUSE/COJ	010-442-42412		07/13/2012	271.13
U Pump It - Gardner Oil	105281	07/13/2012	UP TYLERCOSH/TCSO	010-426-42400		07/13/2012	9,594.22
Election Systems & Software	105181	07/13/2012	T94179/COCLK	010-401-42158		07/13/2012	787.24
Pitney Bowes Global Financi	105241	07/13/2012	8447477/TCSO-JP. 1	010-440-42677		07/13/2012	277.74
County Treasurer's Assoc. of	105166	07/13/2012	REGIS./FULLER, SHARON	010-423-42659		07/13/2012	150.00
Pitney Bowes - Purchase Po	105240	07/13/2012	8000-9090-0176-9145/TCSO	010-401-42111		07/13/2012	67.20
ACE Imagewear	105143	07/13/2012	3719/COJUD	010-442-42150		07/13/2012	39.45
ACE Imagewear	105143	07/13/2012	3719/COJUD	010-442-42150		07/13/2012	39.45
ACE Imagewear	105143	07/13/2012	3719/COJUD	010-442-42150		07/13/2012	39.45
Guardian Force Security Serv	105195	07/13/2012	4862/COCLK	010-442-42412		07/13/2012	240.00
ACE Imagewear	105143	07/13/2012	3719/COJUD	010-442-42150		07/13/2012	39.45
ACE Imagewear	105143	07/13/2012	3719/COJUD	010-442-42150		07/13/2012	39.45
Deep East Texas Council of G	105171	07/13/2012	APRIL 12/LUNCHEON	010-401-42233		07/13/2012	9.00
East Texas Regional Water Pl	105178	07/13/2012	INV.#43 MEMB. DUES/COJU	010-401-42178		07/13/2012	300.00

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
GT Distributors, Inc.	105194	07/13/2012	003939/TCSO	010-426-42182		07/13/2012	364.30
Allan Shivers Library and Mu	105146	07/13/2012	3RD QTR ALLOTMENT/COAU	010-401-42649		07/13/2012	28,750.00
Deep East Texas Council of G	105171	07/13/2012	JUNE 2012/LUNCHEON	010-401-42233		07/13/2012	32.00
Sullivan's Hardware	105260	07/13/2012	JUNE 2012/COJUD	010-442-42412		07/13/2012	187.29
Deep East Texas Council of G	105171	07/13/2012	MAY 2012/LUNCHEON	010-401-42233		07/13/2012	99.00
Professional Safety Systems	105244	07/13/2012	INV.#PSS-122052	010-426-42653		07/13/2012	250.00
Woodville Volunteer Fire De	105301	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	3,458.75
Warren Volunteer Fire Dept.	105291	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	4,528.75
Fred Volunteer Fire Dept.	105189	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	2,541.25
Spurger Volunteer Fire Dept.	105256	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	4,042.50
Dam B Volunteer Fire Dept.	105169	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	3,249.58
Wildwood Volunteer Fire De	105297	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	1,312.00
White Tail Ridge Fire Dept.	105296	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	242.50
Ivanhoe Volunteer Fire Dept.	105206	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	2,899.25
Shady Grove Volunteer Fire	105253	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	1,425.33
Colmesneil Volunteer Fire D	105162	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	5,839.13
Dam B Volunteer Fire Dept.	105169	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	5,960.25
Spurger Volunteer Fire Dept.	105256	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	7,954.87
Woodville Volunteer Fire De	105301	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	7,489.13
Ivanhoe Volunteer Fire Dept.	105206	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	4,627.13
Colmesneil Volunteer Fire D	105162	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	9,865.79
Warren Volunteer Fire Dept.	105291	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	3,769.88
Shady Grove Volunteer Fire	105253	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	2,646.23
Fred Volunteer Fire Dept.	105189	07/13/2012	STATE REIMB/WILDFIRE PRO	010-401-42915		07/13/2012	3,611.25
FP Mailing Solutions	105188	07/13/2012	500065071/TAX	010-401-42111		07/13/2012	105.00
Noble Industrial Supply Corp	105231	07/13/2012	34557/TCSO	010-427-42108		07/13/2012	664.65
Deep East Texas Council of G	105172	07/13/2012	MEMB. DUES/COJUD	010-401-42650		07/13/2012	1,673.62
Dell Marketing L.P.	105173	07/13/2012	006789522/COMMISSIONER	010-453-43210		07/13/2012	449.00
Dell Marketing L.P.	105173	07/13/2012	006789522/TCSO	010-453-43210		07/13/2012	319.21
OFFICE OF THE A.G. CHILD S	1	07/13/2012	case#11346400	010-21300		07/13/2012	191.50
GULF EMPLOYEES CREDIT U	105135	07/13/2012	Julius A. Walston - acct# 100	010-21300		07/13/2012	75.00
OFFICE OF THE A.G. CHILD S	1	07/13/2012	CS	010-21300		07/13/2012	200.00
OFFICE OF THE A.G. CHILD S	1	07/13/2012	CS	010-21300		07/13/2012	143.00
OFFICE OF THE A.G. CHILD S	1	07/13/2012	CS	010-21300		07/13/2012	312.58
OFFICE OF THE A.G. CHILD S	1	07/13/2012	CS	010-21300		07/13/2012	175.00
Tyler County Payroll	105136	07/13/2012	FICA	010-21300		07/13/2012	11,073.16
Tyler County Payroll	105136	07/13/2012	Federal Withholding	010-21300		07/13/2012	9,095.79
Tyler County Payroll	105136	07/13/2012	Medicare	010-21300		07/13/2012	3,087.62
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	010-29999		07/13/2012	80,481.77
Fund 010 - GENERAL FUND Total:							294,693.47
Fund: 021 - ROAD & BRIDGE I							
Bryan & Bryan Asphalt Road	105155	07/13/2012	TYLER1/PCT. 1	021-000-42160		07/13/2012	14,864.85
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT1/PCT. 1	021-000-42400		07/13/2012	2,486.47

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Walling Signs & Graphics/Pa	105289	07/13/2012	INV.#13563/PCT. 1	021-000-42998		07/13/2012	70.00
Lakes areas Septic & Sludge	105211	07/13/2012	INV.#23594/PCT. 1	021-000-42510		07/13/2012	25.00
Lakes areas Septic & Sludge	105211	07/13/2012	INV.#23636/PCT. 1	021-000-42510		07/13/2012	25.00
Texas Association of Countie	105264	07/13/2012	PCT. 1	021-000-40140		07/13/2012	130.29
Allison Chevrolet / Jasper	105147	07/13/2012	INSPECTION/PCT. 1	021-000-42425		07/13/2012	14.50
A T & T / Phone Lines / Carol	105140	07/13/2012	PCT. 1	021-000-42500		07/13/2012	52.22
Timberman's Supply	105268	07/13/2012	12023/PCT. 1	021-000-42425		07/13/2012	309.43
Parker Lumber - Woodville	105237	07/13/2012	22700/PCT. 1	021-000-42425		07/13/2012	53.59
Entergy	105184	07/13/2012	451030/PCT. 1	021-000-42510		07/13/2012	176.70
Tyler County Auto Parts/NAP	105275	07/13/2012	7050/PCT. 1	021-000-42425		07/13/2012	59.37
Modica Bros.	105222	07/13/2012	JUNE 2012/PCT. 1	021-000-42401		07/13/2012	1,237.66
WalMart Community/GECRB	105290	07/13/2012	5371/PCT. 1	021-000-42998		07/13/2012	87.55
U Pump It - Gardner Oil	105281	07/13/2012	UP TYCOPCT1/PCT. 1	021-000-42400		07/13/2012	337.72
A-1 Johnny Portable Toilets	105142	07/13/2012	INV.#91701/PCT. 1	021-000-42510		07/13/2012	35.00
Kay Electronics, Inc.	105209	07/13/2012	INV.#INV56971/PCT. 1	021-000-42425		07/13/2012	381.75
OFFICE OF THE A.G. CHILD S	1	07/13/2012	CS	021-21300		07/13/2012	250.00
Tyler County Payroll	105136	07/13/2012	FICA	021-21300		07/13/2012	1,112.15
Tyler County Payroll	105136	07/13/2012	Federal Withholding	021-21300		07/13/2012	923.40
Tyler County Payroll	105136	07/13/2012	Medicare	021-21300		07/13/2012	310.08
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	021-29999		07/13/2012	7,976.04
Fund 021 - ROAD & BRIDGE I Total:							30,918.77
Fund: 022 - ROAD & BRIDGE II							
Martin's True Value Hardwar	105219	07/13/2012	INV.#14573/PCT. 2	022-000-42425		07/13/2012	9.52
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT2/PCT. 2	022-000-42400		07/13/2012	3,503.08
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT2/PCT. 2	022-000-42400		07/13/2012	1,450.40
Jerry's Saw Shop	105208	07/13/2012	INV. #025835/PCT. 2	022-000-42425		07/13/2012	44.60
Jerry's Saw Shop	105208	07/13/2012	INV.#025968/PCT. 2	022-000-42425		07/13/2012	154.70
Econo Signs, LLC	105180	07/13/2012	75979PCT1&2/PCT. 2	022-000-42425		07/13/2012	73.99
O'Reilly Automotive, Inc.	105235	07/13/2012	591682/PCT. 2	022-000-42425		07/13/2012	88.97
O'Reilly Automotive, Inc.	105235	07/13/2012	591682/PCT. 2	022-000-42425		07/13/2012	10.98
O'Reilly Automotive, Inc.	105235	07/13/2012	591682/PCT. 2	022-000-42425		07/13/2012	33.95
Tyler County Tractor	105279	07/13/2012	1347/PCT. 2	022-000-42425		07/13/2012	256.37
Northern Tool & Equipment/	105232	07/13/2012	7003-7057-0016-0100/PCT.	022-000-42425		07/13/2012	75.88
Texas Association of Countie	105264	07/13/2012	PCT. 2	022-000-40140		07/13/2012	104.25
Beaumont Tractor Company,	105150	07/13/2012	TYLE05/PCT. 2	022-000-42425		07/13/2012	415.56
Tools Plus Industries	105270	07/13/2012	INV.#38513/PCT. 2	022-000-42425		07/13/2012	132.07
Nalcom Wireless Communic	105229	07/13/2012	INV.#39715/PCT. 2	022-000-42425		07/13/2012	273.20
Tractor Supply Credit Plan	105271	07/13/2012	6035301202794523/PCT. 2	022-000-42425		07/13/2012	699.99
A T & T / Phone Lines / Carol	105140	07/13/2012	PCT. 2	022-000-42500		07/13/2012	52.22
Tyler County Auto Parts/NAP	105275	07/13/2012	7051/PCT. 2	022-000-42425		07/13/2012	107.91
Horton's Automotive	105200	07/13/2012	6-19-12/PCT. 2	022-000-42425		07/13/2012	573.00
Timberman's Supply	105268	07/13/2012	12024/PCT. 2	022-000-42425		07/13/2012	278.15
Sullivan's Hardware	105260	07/13/2012	JUNE 2012/PCT. 2	022-000-42425		07/13/2012	42.48

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Parker Lumber - Woodville	105237	07/13/2012	22705/PCT. 2	022-000-42425		07/13/2012	98.90
Tyler County Tractor	105279	07/13/2012	1347/PCT. 2	022-000-42425		07/13/2012	1.75
Verizon Wireless	105288	07/13/2012	6997-00001/PCT. 2	022-000-42500		07/13/2012	239.04
Beaumont Tractor Company,	105151	07/13/2012	KUBOTA M108/PCT. 2	022-000-43200		07/13/2012	1,899.00
Consolidated Communicatio	105163	07/13/2012	936-969-2645/0 - PCT. 2	022-000-42500		07/13/2012	7.79
U Pump It - Gardner Oil	105281	07/13/2012	UP TYLERCCP2/PCT. 2	022-000-42400		07/13/2012	414.54
Rural Pipe & Supply	105248	07/13/2012	TYLCO2/PCT. 2	022-000-42161		07/13/2012	1,302.60
Gulf Welding Supply Co.	105196	07/13/2012	030133/PCT 2	022-000-42425		07/13/2012	51.00
Kay Electronics, Inc.	105209	07/13/2012	INV.#INV56971A/PCT. 2	022-000-42425		07/13/2012	381.75
PowerPlan	105242	07/13/2012	87001-13258/PCT. 2	022-000-42425		07/13/2012	3,132.23
D & J Tire, INC	105168	07/13/2012	37013/PCT. 2	022-000-42401		07/13/2012	818.00
D & J Tire, INC	105168	07/13/2012	37013/PCT. 2	022-000-42401		07/13/2012	1,157.00
OFFICE OF THE A.G. CHILD S	1	07/13/2012	CS	022-21300		07/13/2012	225.00
Tyler County Payroll	105136	07/13/2012	FICA	022-21300		07/13/2012	852.60
Tyler County Payroll	105136	07/13/2012	Federal Withholding	022-21300		07/13/2012	743.97
Tyler County Payroll	105136	07/13/2012	Medicare	022-21300		07/13/2012	237.72
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	022-29999		07/13/2012	5,924.82
Fund 022 - ROAD & BRIDGE II Total:							25,868.98
Fund: 023 - ROAD & BRIDGE III							
Martin's True Value Hardwar	105219	07/13/2012	INV.#14559/PCT. 3	023-000-42425		07/13/2012	80.13
Bryan & Bryan Asphalt Road	105155	07/13/2012	TYLER3/PCT. 3	023-000-42160		07/13/2012	14,792.25
Goldstar Products, Inc.	105192	07/13/2012	INV.#0049248/PCT. 3	023-000-42425		07/13/2012	588.00
Lakeway Tire & Service-Jasp	105212	07/13/2012	917/PCT. 3	023-000-42401		07/13/2012	28.50
Lakeway Tire & Service-Jasp	105212	07/13/2012	917/PCT. 3	023-000-42401		07/13/2012	157.45
Lakeway Tire & Service-Jasp	105212	07/13/2012	917/PCT. 3	023-000-42401		07/13/2012	113.95
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT3/PCT. 3	023-000-42400		07/13/2012	2,325.01
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT3/PCT. 3	023-000-42400		07/13/2012	3,526.30
Matheson Tri-Gas INC	105220	07/13/2012	E2314/PCT. 3	023-000-42425		07/13/2012	47.99
Matheson Tri-Gas INC	105220	07/13/2012	E2314/PCT. 3	023-000-42425		07/13/2012	21.60
The Railroad Yard, Inc.	105267	07/13/2012	INV.#141803/PCT. 3	023-000-42161		07/13/2012	8,981.80
O'Reilly Automotive, Inc.	105235	07/13/2012	594754/PCT. 3	023-000-42425		07/13/2012	231.10
Staples Credit Plan	105258	07/13/2012	6035517820773694/PCT. 3	023-000-42998		07/13/2012	119.95
Timberman's Supply	105268	07/13/2012	12025/PCT. 3	023-000-42425		07/13/2012	143.76
Timberman's Supply	105268	07/13/2012	12025/PCT. 3	023-000-42425		07/13/2012	848.74
Texas Association of Countie	105264	07/13/2012	PCT. 3	023-000-40140		07/13/2012	155.52
A T & T / Phone Lines / Carol	105140	07/13/2012	PCT. 3	023-000-42500		07/13/2012	52.21
Tyler County Auto Parts/NAP	105275	07/13/2012	7052/PCT. 3	023-000-42425		07/13/2012	50.66
Tyler County Auto Parts/NAP	105275	07/13/2012	7052/PCT. 3	023-000-42425		07/13/2012	133.00
Tyler County Auto Parts/NAP	105275	07/13/2012	7052/PCT. 3	023-000-42425		07/13/2012	37.00
Tyler County Auto Parts/NAP	105275	07/13/2012	7052/PCT. 3	023-000-42425		07/13/2012	8.99
Tyler County Auto Parts/NAP	105275	07/13/2012	7052/PCT. 3	023-000-42425		07/13/2012	236.44
Triple Blade & Steel	105272	07/13/2012	INV.#6008/PCT. 3	023-000-42425		07/13/2012	640.08
Entergy	105184	07/13/2012	649486/PCT. 3	023-000-42510		07/13/2012	254.84

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Modica Bros.	105222	07/13/2012	JUNE 2012/PCT. 3	023-000-42401		07/13/2012	392.28
Verizon Wireless	105284	07/13/2012	6997-00003/PCT. 3	023-000-42500		07/13/2012	376.54
U Pump It - Gardner Oil	105281	07/13/2012	UP TYCOPCT3/PCT. 3	023-000-42400		07/13/2012	70.96
Kay Electronics, Inc.	105209	07/13/2012	INV.#INV86971/PCT. 3	023-000-42425		07/13/2012	381.75
PowerPlan	105242	07/13/2012	8850494392/PCT. 3	023-000-42425		07/13/2012	218.40
PowerPlan	105242	07/13/2012	8850494392/PCT. 3	023-000-42425		07/13/2012	53.78
Billy Williams Trucking	105153	07/13/2012	6-7-12/PCT. 3	023-000-42160		07/13/2012	1,270.04
Mustang Machinery Compan	105227	07/13/2012	0792920/PCT. 3	023-000-42425		07/13/2012	283.46
Interstate Billing Service, INC	105205	07/13/2012	120677/PCT. 3	023-000-42425		07/13/2012	67.02
Tyler County Payroll	105136	07/13/2012	FICA	023-21300		07/13/2012	1,177.58
Tyler County Payroll	105136	07/13/2012	Federal Withholding	023-21300		07/13/2012	800.54
Tyler County Payroll	105136	07/13/2012	Medicare	023-21300		07/13/2012	328.34
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	023-29999		07/13/2012	8,783.70
Fund 023 - ROAD & BRIDGE III Total:							47,779.66
Fund: 024 - ROAD & BRIDGE IV							
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT4/PCT. 4	024-000-42400		07/13/2012	5,114.64
Gardner Oil, Inc.	105190	07/13/2012	TYCO PCT4/PCT. 4	024-000-42400		07/13/2012	115.00
The Railroad Yard, Inc.	105267	07/13/2012	INV.#141803/PCT. 4	024-000-42161		07/13/2012	8,981.81
Ellis Truck & Trailer Parts	105183	07/13/2012	0100151/PCT. 4	024-000-42425		07/13/2012	43.19
Mott Wholesale, Inc.	105223	07/13/2012	INV.#18317/PCT. 4	024-000-42425		07/13/2012	286.73
Mott Wholesale, Inc.	105223	07/13/2012	INV.#18496/PCT. 4	024-000-42425		07/13/2012	187.29
Staples Credit Plan	105258	07/13/2012	6035517820773694/PCT. 4	024-000-42998		07/13/2012	119.95
Texas Association of Countie	105264	07/13/2012	PCT. 4	024-000-40140		07/13/2012	125.95
Allison Chevrolet / Jasper	105147	07/13/2012	INV.#31992/PCT. 4	024-000-42425		07/13/2012	14.50
A T & T / Phone Lines / Carol	105140	07/13/2012	PCT. 4	024-000-42500		07/13/2012	52.21
Timberman's Supply	105268	07/13/2012	12026/PCT. 4	024-000-42425		07/13/2012	374.49
Overstreet, Susan M.	105236	07/13/2012	STMT.#6/PCT. 4	024-000-42160		07/13/2012	1,824.00
Entergy	105184	07/13/2012	485012/PCT. 4	024-000-42510		07/13/2012	61.94
Verizon Wireless	105283	07/13/2012	5093-00001/PCT. 4	024-000-42500		07/13/2012	159.96
Pate's Collision	105238	07/13/2012	2011 FORD 250/PCT. 4	024-000-42425		07/13/2012	9,000.00
Telstar Specialty Products	105263	07/13/2012	INV.#7404/PCT. 4	024-000-42998		07/13/2012	124.20
U Pump It - Gardner Oil	105281	07/13/2012	UP TYCOPCT4/PCT. 4	024-000-42400		07/13/2012	155.72
Rural Pipe & Supply	105248	07/13/2012	TYLER4/PCT. 4	024-000-42161		07/13/2012	2,131.80
Kay Electronics, Inc.	105209	07/13/2012	INV.#INV56971C/PCT. 4	024-000-42425		07/13/2012	381.75
PowerPlan	105242	07/13/2012	87001-13241/PCT. 4	024-000-42425		07/13/2012	421.44
PowerPlan	105242	07/13/2012	87001-13241/PCT. 4	024-000-42425		07/13/2012	4,018.62
Tyler County Payroll	105136	07/13/2012	FICA	024-21300		07/13/2012	1,019.68
Tyler County Payroll	105136	07/13/2012	Federal Withholding	024-21300		07/13/2012	959.56
Tyler County Payroll	105136	07/13/2012	Medicare	024-21300		07/13/2012	284.34
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	024-29999		07/13/2012	7,613.12
Fund 024 - ROAD & BRIDGE IV Total:							43,571.89
Fund: 029 - BENEVOLENCE FUND							
Woodville Florist & Gift Shop	105299	07/13/2012	INV.#004256/TREAS.	029-000-42684		07/13/2012	70.00

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Flower Shop	105186	07/13/2012	BRANTLY, DARLENE/TREAS.	029-000-42684		07/13/2012	125.00
Fund 029 - BENEVOLENCE FUND Total:							195.00
Fund: 031 - COUNTY CLERK RMP							
Net Data Corp.	105230	07/13/2012	TYL900057/COCLK	031-000-42695		07/13/2012	225.00
Texas Association of Countie	105264	07/13/2012	COUNTY CLERK ARCHIVE	031-000-40140		07/13/2012	14.57
Tyler County Payroll	105136	07/13/2012	FICA	031-21300		07/13/2012	70.99
Tyler County Payroll	105136	07/13/2012	Federal Withholding	031-21300		07/13/2012	3.68
Tyler County Payroll	105136	07/13/2012	Medicare	031-21300		07/13/2012	19.80
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	031-29999		07/13/2012	612.07
Fund 031 - COUNTY CLERK RMP Total:							946.11
Fund: 034 - DISTRICT CLERK RMP							
Scott Merriman, INC.	105250	07/13/2012	TY02/DSCLK	034-000-48010		07/13/2012	870.52
Fund 034 - DISTRICT CLERK RMP Total:							870.52
Fund: 036 - LIBRARY FUND							
Lexis Nexis	105216	07/13/2012	1396TR/DSJUD	036-000-48007		07/13/2012	46.00
Fund 036 - LIBRARY FUND Total:							46.00
Fund: 037 - T C COLLECTION CENTER							
Lakeway Tire & Service-Jasp	105212	07/13/2012	1174/COLL. CTR.	037-000-42425		07/13/2012	32.00
IESI Hardin County Landfill	105201	07/13/2012	052032696/COLL. CTR.	037-000-42177		07/13/2012	2,419.80
IESI Hardin County Landfill	105201	07/13/2012	052032696/COLL. CTR.	037-000-42177		07/13/2012	2,037.60
Texas Association of Countie	105264	07/13/2012	TC COLLECTION SITE	037-000-40140		07/13/2012	39.78
A T & T / Phone Lines / Carol	105140	07/13/2012	COLLECTION CENTER	037-000-42510		07/13/2012	27.54
Timberman's Supply	105268	07/13/2012	12028/COLL. CTR.	037-000-42425		07/13/2012	11.25
Sullivan's Hardware	105260	07/13/2012	JUNE 2012/COLL. CTR.	037-000-42425		07/13/2012	42.01
WalMart Community/GEGRB	105290	07/13/2012	2157/COLL. CTR.	037-000-42998		07/13/2012	21.78
Entergy	105184	07/13/2012	5082/COLL. CTR.	037-000-42510		07/13/2012	99.36
Fortenberry Electric	105187	07/13/2012	CHANGE LGT. FIXTURES/COL	037-000-42510		07/13/2012	100.00
Gardner Oil, Inc.	105190	07/13/2012	TYCO COLLECTION/COLL. CT	037-000-42400		07/13/2012	1,225.37
Parker Lumber - Woodville	105237	07/13/2012	22725/COLL. CTR.	037-000-42425		07/13/2012	24.99
Tyler County Payroll	105136	07/13/2012	FICA	037-21300		07/13/2012	260.11
Tyler County Payroll	105136	07/13/2012	Federal Withholding	037-21300		07/13/2012	217.96
Tyler County Payroll	105136	07/13/2012	Medicare	037-21300		07/13/2012	72.54
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	037-29999		07/13/2012	1,966.70
Fund 037 - T C COLLECTION CENTER Total:							8,598.79
Fund: 044 - COURTHOUSE SECURITY							
Texas Association of Countie	105264	07/13/2012	COURTHOUSE SECURITY	044-000-40140		07/13/2012	9.15
A T & T / Phone Lines / Carol	105140	07/13/2012	COURTHOUSE SECURITY	044-000-42510		07/13/2012	27.54
Tyler County Payroll	105136	07/13/2012	FICA	044-21300		07/13/2012	46.80
Tyler County Payroll	105136	07/13/2012	Federal Withholding	044-21300		07/13/2012	11.25
Tyler County Payroll	105136	07/13/2012	Medicare	044-21300		07/13/2012	13.06
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	044-29999		07/13/2012	413.32
Fund 044 - COURTHOUSE SECURITY Total:							521.12

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Fund: 045 - COUNTY-RMP							
Net Data Corp.	105230	07/13/2012	TYL900057/COCLK	045-000-48000		07/13/2012	225.00
Fund 045 - COUNTY-RMP Total:							225.00
Fund: 049 - C D A TRUST							
West Magnolia/Restiution	105293	07/13/2012	BARLOW, CLINTON/CDA	049-000-42908		07/13/2012	105.00
Brookshire Brothers/Resituti	105154	07/13/2012	MCGOUGH, CHAZ/CDA	049-000-42908		07/13/2012	50.00
Brookshire Brothers/Resituti	105154	07/13/2012	VAUGHN, WILLIAM/CDA	049-000-42908		07/13/2012	265.67
Brookshire Brothers/Resituti	105154	07/13/2012	TROTTER, ROGER/CDA	049-000-42908		07/13/2012	118.00
Babin, Brian	105148	07/13/2012	WARNER, RICHARD/CDA	049-000-42908		07/13/2012	120.00
The Medicine Shoppe / Woo	105266	07/13/2012	HUERTA, IMELDA/CDA	049-000-42908		07/13/2012	62.68
The Medicine Shoppe / Woo	105266	07/13/2012	BRANDIN, JOSEPH/CDA	049-000-42908		07/13/2012	34.00
Country Food Mart	105165	07/13/2012	COWETT, DARLA/CDA	049-000-42908		07/13/2012	113.02
Country Food Mart	105165	07/13/2012	FOSTER, CRAIG/CDA	049-000-42908		07/13/2012	60.00
Tyler County Sheriff Depart	105278	07/13/2012	BARLOW, CLINTON/CDA	049-000-42908		07/13/2012	50.00
Barlow, Clinton	105149	07/13/2012	OVERPAYMENT/CDA	049-000-42908		07/13/2012	120.00
Dover, Bill L.	105176	07/13/2012	WILSON, ARTHUR B. III/CDA	049-000-42908		07/13/2012	114.39
Fund 049 - C D A TRUST Total:							1,212.76
Fund: 050 - C D A FEES							
Tyler County Payroll	105136	07/13/2012	FICA	050-21300		07/13/2012	19.96
Tyler County Payroll	105136	07/13/2012	Medicare	050-21300		07/13/2012	5.56
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	050-29999		07/13/2012	181.16
Fund 050 - C D A FEES Total:							206.68
Fund: 053 - ADULT PROBATION							
CNA Surety	105161	07/13/2012	BOND #060118164354/CSCD	053-000-42602		07/13/2012	175.00
Walling Signs & Graphics/Pa	105289	07/13/2012	INV.#13528/CSCD	053-000-42104		07/13/2012	116.00
Story-Wright	105259	07/13/2012	101851/CSCD	053-000-42104		07/13/2012	67.36
Story-Wright	105259	07/13/2012	101851/CSCD	053-000-42104		07/13/2012	53.68
Tyler County	105274	07/13/2012	JULY 2012/CSCD	053-434-42629		07/13/2012	2,000.00
Oce' Imagistics Inc.	105234	07/13/2012	SR3409/CSCD	053-000-42104		07/13/2012	25.00
Corrections Software Solutio	105164	07/13/2012	INV.#25942/CSCD	053-000-42602		07/13/2012	995.00
Texas Association of Countie	105264	07/13/2012	ADULT PROBATION	053-000-40140		07/13/2012	163.36
Quill Corporation	105245	07/13/2012	C2772734/CSCD	053-000-42104		07/13/2012	211.02
Quill Corporation	105245	07/13/2012	C2772734/CSCD	053-000-42104		07/13/2012	301.44
LEAF	105214	07/13/2012	100-1539477-001/CSCD	053-000-42104		07/13/2012	100.00
A T & T / Phone Lines / Carol	105140	07/13/2012	ADULT PROBATION	053-000-42510		07/13/2012	30.00
Music Mountain Water Com	105224	07/13/2012	51092000/CSCD	053-000-42104		07/13/2012	50.45
Alere Toxicology Services, In	105145	07/13/2012	MACK, TRABYAN/CSCD	053-000-42647		07/13/2012	15.00
Alere Toxicology Services, In	105145	07/13/2012	LAND, ANTHONY/CSCD	053-000-42647		07/13/2012	15.00
Alere Toxicology Services, In	105145	07/13/2012	SAPH, ERIC/CSCD	053-000-42647		07/13/2012	15.00
Tyler County Payroll	105136	07/13/2012	FICA	053-21300		07/13/2012	1,016.44
Tyler County Payroll	105136	07/13/2012	Federal Withholding	053-21300		07/13/2012	1,066.19
Tyler County Payroll	105136	07/13/2012	Medicare	053-21300		07/13/2012	283.44

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount	
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	053-29999		07/13/2012	7,383.38	
							Fund 053 - ADULT PROBATION Total:	14,082.76
Fund: 054 - JUVENILE PROBATION								
Texas Association of Countie	105264	07/13/2012	JUVENILE PROBATION	054-451-40140		07/13/2012	93.34	
Texas Association of Countie	105264	07/13/2012	JUPRO/SUMMER YTH. PROG.	054-456-40140		07/13/2012	23.94	
WalMart Community/GEGRB	105290	07/13/2012	0824/JUPRO	054-451-42100		07/13/2012	72.25	
Music Mountain Water Com	105226	07/13/2012	82308201/JUPRO	054-451-42100		07/13/2012	35.24	
Canter, Jenifer	105158	07/13/2012	MATH TUTOR/SUMM. YTH.	054-456-42105		07/13/2012	120.00	
Tyler County Payroll	105136	07/13/2012	FICA	054-21300		07/13/2012	1,201.31	
Tyler County Payroll	105136	07/13/2012	Federal Withholding	054-21300		07/13/2012	1,067.39	
Tyler County Payroll	105136	07/13/2012	Medicare	054-21300		07/13/2012	334.98	
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	054-29999		07/13/2012	9,282.47	
							Fund 054 - JUVENILE PROBATION Total:	12,230.92
Fund: 073 - JUSTICE COURT TECHNOLOGY FUND								
Verizon Wireless	105287	07/13/2012	5066-00001/BROADBAND	073-000-42101		07/13/2012	48.59	
							Fund 073 - JUSTICE COURT TECHNOLOGY FUND Total:	48.59
Fund: 076 - EMERGENCY OPERATIONS CENTER								
Indoff Office Supplies	105202	07/13/2012	183922/EOC	076-000-42100		07/13/2012	171.86	
Texas Association of Countie	105264	07/13/2012	EMERGENCY MGMT.	076-000-40140		07/13/2012	50.47	
Parker Lumber - Woodville	105237	07/13/2012	22735/EOC	076-000-42663		07/13/2012	2.76	
A T & T / Phone Lines / Carol	105140	07/13/2012	EMERGENCY MGMT.	076-000-42500		07/13/2012	364.35	
U Pump It - Gardner Oil	105281	07/13/2012	UP TYCO EMER MGT2/EOC	076-000-42416		07/13/2012	213.48	
Data Collection Specialists, I	105170	07/13/2012	INV.#8856/EOC	076-000-42100		07/13/2012	67.26	
Tyler County Payroll	105136	07/13/2012	FICA	076-21300		07/13/2012	219.02	
Tyler County Payroll	105136	07/13/2012	Federal Withholding	076-21300		07/13/2012	144.59	
Tyler County Payroll	105136	07/13/2012	Medicare	076-21300		07/13/2012	61.08	
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	076-29999		07/13/2012	1,706.52	
							Fund 076 - EMERGENCY OPERATIONS CENTER Total:	3,001.39
Fund: 089 - TYLER COUNTY NUTRITION CENTER								
Lifetime Products, Inc.	105217	07/13/2012	INV.#1685339/NUTR. CTR.	089-000-43200		07/13/2012	1,299.98	
DirecTV	105175	07/13/2012	035535115/NUTR. CTR.	089-000-42510		07/13/2012	89.99	
Parker Lumber - Woodville	105237	07/13/2012	22700/NUTR. CTR.	089-000-42410		07/13/2012	271.84	
Parker Lumber - Woodville	105237	07/13/2012	22725/NUTR. CTR.	089-000-42410		07/13/2012	21.57	
Entergy	105184	07/13/2012	451094/NUTR. CTR.	089-000-42510		07/13/2012	1,002.18	
WalMart Community/GEGRB	105290	07/13/2012	5371/PCT. 1	089-000-42204		07/13/2012	62.81	
Tyler County Payroll	105136	07/13/2012	FICA	089-21300		07/13/2012	29.12	
Tyler County Payroll	105136	07/13/2012	Medicare	089-21300		07/13/2012	8.12	
TYLER COUNTY PAYROLL	105139	07/13/2012	PAYROLL TRANSFER	089-29999		07/13/2012	244.58	
							Fund 089 - TYLER COUNTY NUTRITION CENTER Total:	3,030.19
Fund: 100 - DETCOG SOCIAL SERVICES BLOCK G								
TYLER COUNTY PAYROLL	105139	07/13/2012	net salaries ppd 05/25/2012	100-29999		07/13/2012	2.76	
							Fund 100 - DETCOG SOCIAL SERVICES BLOCK G Total:	2.76

CHECK REGISTER

Payable Dates: 7/13/2012 - 7/13/2012

Vendor Name	Payment Number	Post Date	Description (Item)	Account Number	Project Account Key	Post Date	Amount
Fund: 111 - COURTHOUSE RESTORATION							
Whelan, Robert William	105295	07/13/2012	WINDOW RESTOR./COJUD	111-000-48011		07/13/2012	75.00
Whelan, Robert William	105295	07/13/2012	WINDOW RESTOR./COJUD	111-000-48011		07/13/2012	275.00
Parker Lumber - Woodville	105237	07/13/2012	22725/WINDOW RESTORATI	111-000-42412		07/13/2012	188.48
Tyler County Auto Parts/NAP	105275	07/13/2012	7053/COURTHOUSE	111-000-42412		07/13/2012	16.69
Sullivan's Hardware	105260	07/13/2012	JUNE 2012/COURTHOUSE RE	111-000-48011		07/13/2012	113.71
Fund 111 - COURTHOUSE RESTORATION Total:							668.88
Grand Total:							488,720.24

Report Summary

Fund Summary

Fund	Payment Amount
010 - GENERAL FUND	294,693.47
021 - ROAD & BRIDGE I	30,918.77
022 - ROAD & BRIDGE II	25,868.98
023 - ROAD & BRIDGE III	47,779.66
024 - ROAD & BRIDGE IV	43,571.89
029 - BENEVOLENCE FUND	195.00
031 - COUNTY CLERK RMP	946.11
034 - DISTRICT CLERK RMP	870.52
036 - LIBRARY FUND	46.00
037 - T C COLLECTION CENTER	8,598.79
044 - COURTHOUSE SECURITY	521.12
045 - COUNTY-RMP	225.00
049 - C D A TRUST	1,212.76
050 - C D A FEES	206.68
053 - ADULT PROBATION	14,082.76
054 - JUVENILE PROBATION	12,230.92
073 - JUSTICE COURT TECHNOLOGY FUND	48.59
076 - EMERGENCY OPERATIONS CENTER	3,001.39
089 - TYLER COUNTY NUTRITION CENTER	3,030.19
100 - DETCOG SOCIAL SERVICES BLOCK G	2.76
111 - COURTHOUSE RESTORATION	668.88
Grand Total:	488,720.24

Account Summary

Account Number	Account Name	Payment Amount
010-21300	PAYROLL LIABILITIES	24,353.65
010-29999	Due To Other Funds	80,481.77
010-401-40140	UNEMPLOYMENT INSUR	1,395.02
010-401-42111	POSTAGE FOR POSTAGE	710.98
010-401-42158	ELECTION EXPENSE	989.11
010-401-42178	CONTINGENCY FOR MIS	3,430.35
010-401-42233	DETCOG TRAVEL	140.00
010-401-42352	TC NUTRITION SERVICES	3,750.00
010-401-42519	PROBATION TELEPHONE	218.34
010-401-42616	ADVERTISING	72.00
010-401-42649	ALLEN SHIVERS LIBRARY	28,750.00
010-401-42650	ASSOCIATION DUES	1,673.62
010-401-42667	JAIL NEEDS ANALYSIS	4,022.33
010-401-42668	INDEPENDENT AUDIT	22,650.00
010-401-42915	WILDFIRE REIMBURSEM	75,463.57

Account Summary

Account Number	Account Name	Payment Amount
010-401-48000	MISCELLANEOUS EXPEN	284.00
010-402-42100	OFFICE SUPPLIES	220.92
010-402-42500	TELEPHONE	186.91
010-402-42659	TRAVEL & EDUCATION	152.07
010-405-42100	OFFICE SUPPLIES	348.93
010-405-42500	TELEPHONE	157.76
010-407-42100	OFFICE SUPPLIES	734.60
010-407-42500	TELEPHONE	57.23
010-407-42659	TRAVEL & EDUCATION	30.00
010-408-42689	GRAND JURORS	80.00
010-409-42500	TELEPHONE	27.54
010-411-42500	TELEPHONE	160.83
010-411-42661	TRAINING & EDUCATION	874.60
010-415-42634	COURT APPOINTED ATT	2,475.00
010-419-42500	TELEPHONE	192.78
010-420-42500	TELEPHONE	287.13
010-421-42500	TELEPHONE	140.41
010-422-42100	OFFICE SUPPLIES	11.99
010-422-42500	TELEPHONE	55.08
010-423-42100	OFFICE SUPPLIES	201.86
010-423-42500	TELEPHONE	27.54
010-423-42659	TRAVEL & EDUCATION	150.00
010-426-42100	OFFICE SUPPLIES	1,072.85
010-426-42182	DEPUTIES SUPPLIES	427.41
010-426-42400	GAS, OIL, GREASE	9,899.42
010-426-42401	TIRES, TUBES	1,634.35
010-426-42413	REPAIRS TO VEHICLES	1,575.85
010-426-42500	TELEPHONE	2,041.73
010-426-42653	CAMERA & FILM	250.00
010-426-42656	ANIMAL CONTROL	203.90
010-426-42659	TRAVEL & EDUCATION	421.00
010-427-42108	JAIL SUPPLIES	3,616.18
010-427-42900	BONDS	142.00
010-430-42500	TELEPHONE	108.57
010-430-42502	TELEPHONE - PARKS &	27.54
010-430-42503	TELEPHONE - DRIVERS LI	55.08
010-439-42100	OFFICE SUPPLIES	66.00
010-439-42500	TELEPHONE	55.08
010-440-42101	SUPPLIES	1,150.62
010-440-42350	SERVICE CONTRACTS	161.61
010-440-42353	SUPPORT SERVICES	1,070.85
010-440-42677	EQUIPMENT LEASE	1,792.11

Account Summary

Account Number	Account Name	Payment Amount
010-442-42106	JANITORS SUPPLIES	478.62
010-442-42150	UNIFORMS	197.25
010-442-42220	WHEAT BUILDING LEASE	1,000.00
010-442-42411	REPAIRS AT JUSTICE CEN	560.44
010-442-42412	REPAIRS TO COURTHOU	2,899.26
010-442-42422	ELEVATOR REPAIRS	81.03
010-442-42511	UTILITIES-JUSTICE CENT	3,699.67
010-442-42512	UTILITIES-WHEAT BUILDI	301.68
010-442-42515	UTILITIES-COURTHOUSE	1,573.57
010-442-42516	UTILITIES-BEST BUILDIN	599.74
010-442-42517	UTILITIES-TAX OFFICE	524.00
010-453-43210	OFFICE EQUIPMENT	2,048.14
021-000-40140	UNEMPLOYMENT INSUR	130.29
021-000-42160	ROAD MATERIAL	14,864.85
021-000-42400	GAS, OIL, GREASE	2,824.19
021-000-42401	TIRES, TUBES	1,237.66
021-000-42425	MACHINERY MAINTENA	818.64
021-000-42500	TELEPHONE	52.22
021-000-42510	UTILITIES	261.70
021-000-42998	MISCELLANEOUS SUPPLI	157.55
021-21300	PAYROLL LIABILITIES	2,595.63
021-29999	Due To Other Funds	7,976.04
022-000-40140	UNEMPLOYMENT INSUR	104.25
022-000-42161	CULVERTS	1,302.60
022-000-42400	GAS, OIL, GREASE	5,368.02
022-000-42401	TIRES, TUBES	1,975.00
022-000-42425	MACHINERY MAINTENA	6,936.95
022-000-42500	TELEPHONE	299.05
022-000-43200	PURCHASE OF EQUIPME	1,899.00
022-21300	PAYROLL LIABILITIES	2,059.29
022-29999	Due To Other Funds	5,924.82
023-000-40140	UNEMPLOYMENT INSUR	155.52
023-000-42160	ROAD MATERIAL	16,062.29
023-000-42161	CULVERTS	8,981.80
023-000-42400	GAS, OIL, GREASE	5,922.27
023-000-42401	TIRES, TUBES	692.18
023-000-42425	MACHINERY MAINTENA	4,071.90
023-000-42500	TELEPHONE	428.75
023-000-42510	UTILITIES	254.84
023-000-42998	MISCELLANEOUS SUPPLI	119.95
023-21300	PAYROLL LIABILITIES	2,306.46
023-29999	Due To Other Funds	8,783.70

Account Summary

Account Number	Account Name	Payment Amount
024-000-40140	UNEMPLOYMENT INSUR	125.95
024-000-42160	ROAD MATERIAL	1,824.00
024-000-42161	CULVERTS	11,113.61
024-000-42400	GAS, OIL, GREASE	5,385.36
024-000-42425	MACHINERY MAINTENA	14,728.01
024-000-42500	TELEPHONE	212.17
024-000-42510	UTILITIES	61.94
024-000-42998	MISCELLANEOUS SUPPLI	244.15
024-21300	PAYROLL LIABILITIES	2,263.58
024-29999	Due To Other Funds	7,613.12
029-000-42684	FLORALS	195.00
031-000-40140	UNEMPLOYMENT INSUR	14.57
031-000-42695	PRESERVATION-RMP	225.00
031-21300	PAYROLL LIABILITIES	94.47
031-29999	Due To Other Funds	612.07
034-000-48010	RECORDS PRESERVATIO	870.52
036-000-48007	LIBRARY BOOKS & SUPP	46.00
037-000-40140	UNEMPLOYMENT INSUR	39.78
037-000-42177	CONTAINER HAULS	4,457.40
037-000-42400	GAS, OIL, GREASE	1,225.37
037-000-42425	MACHINERY MAINTENA	110.25
037-000-42510	UTILITIES	226.90
037-000-42998	MISCELLANEOUS SUPPLI	21.78
037-21300	PAYROLL LIABILITIES	550.61
037-29999	Due To Other Funds	1,966.70
044-000-40140	UNEMPLOYMENT INSUR	9.15
044-000-42510	UTILITIES	27.54
044-21300	PAYROLL LIABILITIES	71.11
044-29999	Due To Other Funds	413.32
045-000-48000	MISCELLANEOUS EXPEN	225.00
049-000-42908	RESTITUTION MISC. EXP	1,212.76
050-21300	PAYROLL LIABILITIES	25.52
050-29999	Due To Other Funds	181.16
053-000-40140	UNEMPLOYMENT INSUR	163.36
053-000-42104	SUPPLIES & OPERATING	924.95
053-000-42510	UTILITIES	30.00
053-000-42602	PROFESSIONAL FEES	1,170.00
053-000-42647	CONTRACT SERVICES FO	45.00
053-21300	PAYROLL LIABILITIES	2,366.07
053-29999	Due To Other Funds	7,383.38
053-434-42629	CCP CONTRACT SERV FO	2,000.00
054-21300	PAYROLL LIABILITIES	2,603.68

Account Summary		
Account Number	Account Name	Payment Amount
054-29999	Due To Other Funds	9,282.47
054-451-40140	UNEMPLOYMENT INSUR	93.34
054-451-42100	OFFICE SUPPLIES	107.49
054-456-40140	UNEMPLOYMENT INSUR	23.94
054-456-42105	INSTRUCTIONAL EDUCA	120.00
073-000-42101	SUPPLIES	48.59
076-000-40140	UNEMPLOYMENT INSUR	50.47
076-000-42100	OFFICE SUPPLIES	239.12
076-000-42416	VEHICLE OPERATIONS/	213.48
076-000-42500	TELEPHONE	364.35
076-000-42663	TRAINING & TRAVEL REI	2.76
076-21300	PAYROLL LIABILITIES	424.69
076-29999	Due To Other Funds	1,706.52
089-000-42204	SENIOR ACTIVITIES	62.81
089-000-42410	REPAIRS & MAINTENAN	293.41
089-000-42510	UTILITIES	1,092.17
089-000-43200	PURCHASE OF EQUIPME	1,299.98
089-21300	PAYROLL LIABILITIES	37.24
089-29999	Due To Other Funds	244.58
100-29999	Due To Other Funds	2.76
111-000-42412	RESTORATION EXPENSE	205.17
111-000-48011	COURTHOUSE REPAIRS	463.71
	Grand Total:	488,720.24

Project Account Summary		Payment Amount
Project Account Key		
None		488,720.24
	Grand Total:	488,720.24



Tyler County, TX

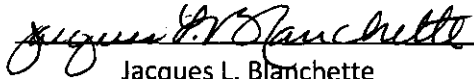
Budget Adjustment Register

Adjustment Detail

Packet: GLPKT00525 - CH

Adjustment Number	Budget Code	Summary Description	Adjustment Date
BA0000032	Budget 2012	COURTHOUSE RESTORATION	7/9/2012
<u>Account Number</u>	<u>Account Name</u>	<u>Allocation Type</u>	<u>Adjustment Description</u>
<u>111-000-42412</u>	RESTORATION EXPENSE	Annual	COURTHOUSE RESTORATION
January: 8,333.33	April: 8,333.33	July: 8,333.33	October: 8,333.33
February: 8,333.33	May: 8,333.33	August: 8,333.33	November: 8,333.33
March: 8,333.33	June: 8,333.33	September: 8,333.33	December: 8,333.37
<u>111-000-48000</u>	MISC. EXPENSE	Annual	COURTHOUSE RESTORATION
January: 4,166.67	April: 4,166.67	July: 4,166.67	October: 4,166.67
February: 4,166.67	May: 4,166.67	August: 4,166.67	November: 4,166.67
March: 4,166.67	June: 4,166.67	September: 4,166.67	December: 4,166.63
<u>111-000-48011</u>	COURTHOUSE REPAIRS	Annual	COURTHOUSE RESTORATION
January: 4,166.67	April: 4,166.67	July: 4,166.67	October: 4,166.67
February: 4,166.67	May: 4,166.67	August: 4,166.67	November: 4,166.67
March: 4,166.67	June: 4,166.67	September: 4,166.67	December: 4,166.63

Approved by the Tyler County Commissioner's Court this 13th of July, 2012.


 Jacques L. Blanchette
 County Judge

ATTEST: 
 Donece Gregory, County Clerk

Summary

Budget	Budget Description	Account	Account Description	Amount
2012	Budget 2012	<u>111-000-42412</u>	RESTORATION EXPENSE	100,000.00
		<u>111-000-48000</u>	MISC. EXPENSE	50,000.00
		<u>111-000-48011</u>	COURTHOUSE REPAIRS	50,000.00
			2012 Total:	200,000.00
			Grand Total:	200,000.00



Tyler County, TX

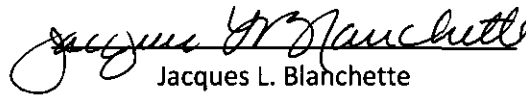
Budget Adjustment Register

Adjustment Detail

Packet: GLPKT00524 - RETI4REMENT CORRECTION

Adjustment Number	Budget Code	Summary Description	Adjustment Date		
BA0000031	Budget 2012	RETIREMENT CORRECTION	7/9/2012		
Account Number	Account Name	Allocation Type	Adjustment Description	Amount	
010-427-40110	RETIREMENT	Annual	RETIREMENT CORRECTION	22,210.00	
January:	1,850.83	April:	1,850.83	October:	1,850.83
February:	1,850.83	May:	1,850.83	November:	1,850.83
March:	1,850.83	June:	1,850.83	December:	1,850.87

Approved by the Tyler County Commissioner's Court this 13th of July, 2012.


 Jacques L. Blanchette
 County Judge

ATTEST: 
 Donece Gregory, County Clerk

Summary

Budget	Budget Description	Account	Account Description	Amount
2012	Budget 2012	<u>010-427-40110</u>	RETIREMENT	22,210.00
			2012 Total:	22,210.00
			Grand Total:	22,210.00



ATTORNEY GENERAL OF TEXAS
GREG ABBOTT
CHILD SUPPORT DIVISION

Donece's Copy
IE TAB 3

June 20, 2012

The Honorable Kim Nagypal
Tyler County District Clerk
100 W Bluff St Rm. 203
Woodville, TX 75979

RE: Two Originals of FY13/14 State Case Registry and Local Customer Service Contract

Dear Ms. Nagypal:

Attached are two originals of the renewal for the FY13/14 State Case Registry/Local Customer Service (SCR/LCS) Contract. Please have both originals signed where indicated.

Also attached is the Incident Response Plan, Attachment G (flagged), which is designed to provide a general reference to both OAG and county staff when a security incident may threaten the confidentiality of OAG data. You will need to submit a new Incident Response Plan even if no changes occurred since the previous contract. Pursuant to contract requirement § 6.4.1.1, please complete the Incident Response Plan and return it along with both signed originals to the following:

Office of the Attorney General
Child Support Division
P. O. Box 12017
Mail Code 062, Attn: Dawn Moss
Austin, Texas 78711-2017

Upon receipt of the two signed originals and the completed Incident Response Plan, the documents will be routed to Alicia G. Key, Deputy Attorney General for Child Support, for signature. After the documents have been signed by all parties, one original will be returned to you for your records. Please be advised, the contract cannot be executed before both signed originals and a current Incident Response Plan have been returned.

If you have questions regarding the execution of this contract, please contact Robert Canales at (512) 460-6283.

Sincerely,

Allen Broussard
Manager, Government Contracts

**Cooperative Agreement
between
The Office of the Attorney General
of the State of Texas
and
Tyler County, Texas**

CONTRACT NO. 13-C0088

1. INTRODUCTION & PURPOSE

- 1.1. This document encompasses furnishing Registry Only court order information relating to Child Support, Protective Orders and Family Violence under the Texas Family Code, Title 4, Subtitle B and Suits Affecting the Parent-Child Relationship under the Texas Family Code, Title 5, Subtitle B for use in the State and Federal Case Registries ("State Case Registry") and local handling of inquiries on (including any necessary research) and receiving information about Child Support Cases where child support payments are remitted to the Texas State Disbursement Unit (TXSDU) ("Local Customer Service"). A County may contract to provide State Case Registry services only. However a county contracting to provide Local Customer Service must also contract to provide State Case Registry.
- 1.2. Tyler ("County") is contracting with the Office of the Attorney General ("OAG") to furnish Registry Only court order information relating to Child Support, Protective Orders and Family Violence under the Texas Family Code, Title 4, Subtitle B and Suits Affecting the Parent-Child Relationship under the Texas Family Code, Title 5, Subtitle B for use in the State and Federal Case Registries.
- 1.3. This Contract and its attachments (all of which are made a part hereof and expressly included herein) is entered into under the authority of Texas Family Code Section 231.002.
- 1.4. The term "OAG Systems" when used in this Contract encompasses the OAG Child Support Case Management System (commonly referred to as TXCSES and TXCSES Web) and any applicable automated systems used by the OAG's Vendor for the TXSDU including all of their subsystems, functions, processes, and security requirements.
- 1.5. Unless specified otherwise in this Contract, all procedures required to be followed by the County will be made available to the County on the OAG child support portal at <http://portal.cs.oag.state.tx.us>.

2. CONTRACT PERIOD

- 2.1. This Contract shall commence on September 1, 2012 and shall terminate on August 31, 2014, unless terminated earlier by provisions of this Contract.

3. REQUIREMENTS OF THE OAG AND THE COUNTY

3.1. State Case Registry Activities

- 3.1.1. County shall provide to OAG new and modified child support court orders entered after the effective date of the Contract for Registry Only child support court order information relating to Suits Affecting the Parent-Child Relationship.
 - 3.1.1.1. County shall use the original court ordered documents to obtain the relevant information for entry to the OAG Systems or may use the "Record of Support" published in the Texas Family Law Manual, or a similar form completed by the District Clerk or Local Registry's office that summarizes the relevant court ordered child support information.

- 3.1.1.2. County must provide, if available, the following data elements:
 - 3.1.1.2.1. participant type (dependent, custodial parent, non-custodial parent)
 - 3.1.1.2.2. family violence indicator, if applicable
 - 3.1.1.2.3. name of each participant (last and first)
 - 3.1.1.2.4. sex code for each participant
 - 3.1.1.2.5. social security number for each custodial parent and non-custodial parent and/or date of birth for each participant
 - 3.1.1.2.6. cause number
 - 3.1.1.2.7. cause county code
 - 3.1.1.2.8. start date of cause
 - 3.1.1.2.9. order modification date
 - 3.1.1.2.10. address lines 1, 2, and 3, City, State, Zip (custodial parent only).
- 3.1.1.3. County shall provide data elements and/or information updates to the OAG Systems for Registry Only child support court orders signed on or after October 1, 1998.
- 3.1.1.4. County shall enter updates on OAG Systems for new case and /or member information provided by the custodial parent, non-custodial parent, employer, court or attorney of record to the County. This includes but is not limited to address information, changes in custody, protective orders, court order terminations of all types, child emancipation, multiple payees or payors, case closure and order transfers.
- 3.1.1.5. County shall endeavor to provide all available new case information necessary to process child support payments received by the State Disbursement Unit within five (5) business days of the "date received time stamp" indicating that the order was received by the District Clerk or Local Registry's office. While this Timeliness Performance Standard is established as a goal for counties rather than a requirement, the OAG intends to monitor and report County performance toward meeting the Standard.
- 3.1.1.6. The provisions of 3.1.1.5 notwithstanding, County shall provide essential new case information necessary to process child support payments received by the State Disbursement Unit within five (5) business days of notification by the Texas TXSDU that a payment was received.
- 3.1.1.7. County shall provide updated information on existing cases within three (3) business days of receipt.
- 3.1.1.8. County shall ensure that the Family Violence Indicator (FVI) is updated on Registry Only cases in TXCSES Web within three (3) business days of a protective order being filed. If a Full Service case exists the county shall provide the local OAG field office with a copy of the protective order within three (3) business days of it being filed.
- 3.1.1.9. County shall provide new and updated case information by data entry directly onto OAG Systems, unless agreed to otherwise in writing by the OAG Contract Manager.
- 3.1.1.10. County shall ensure that payments on cases that have been redirected from the County registry to the TXSDU are paid to the TXSDU and that disbursements on such cases are no longer made by the County. The District Clerk or the Domestic Relations Office (as

applicable) shall send all erroneously received child support payments to the TXSDU within one day of receipt.

3.1.1.11. County agrees that all court orders must direct child support payments to the (TXSDU) in accordance with Section 154.004 of the Texas Family Code and 42 USC 654b of the Code of Federal Regulations. Where the County identifies a pattern of court orders from a particular court or attorney that fail to comply with Section 154.004 of the Texas Family Code and 42 USC 654b of the Code of Federal Regulations, the County will notify the OAG of same.

3.1.1.12. County shall work with the TXSDU to perform the required due diligence to place child support payments into the hands of custodial parents.

3.2. LOCAL CUSTOMER SERVICE

3.2.1. County Customer Service Unit Resources and Services

3.2.1.1. The term "Child Support Cases" when used in this Section and its Subsections means: Registry Only cases (a Registry Only case is a case where the payment is remitted to the State Disbursement Unit by an employer pursuant to an original order signed on or after January 1, 1994) and all IV-D cases (also known as "Full Service Cases").

3.2.1.2. County shall provide the resources necessary to accomplish the following allowable categories of customer service activity on Child Support Cases in accordance with the requirements of the Confidentiality and Security Section below: Payment Inquiry, Payment Research, Employer Payment Related Calls, OAG Payment Related Calls, Withholding Inquiry (Employer, Custodial Parent, Non-Custodial Parent).

3.2.1.2.1. These activities include but are not limited to:

3.2.1.2.1.1. Researching payments on Child Support Cases that should have been but were not received by the OAG.

3.2.1.2.1.2. Researching disbursements on Child Support Cases that should have been but were not received by the custodial parent.

3.2.1.2.1.3. Providing payment records on Child Support Cases to the court, the guardian ad litem for the child, the custodial and non-custodial parent and their attorneys, a person authorized by the custodial or non-custodial parent to have the payment history information, and a District or County attorney for purposes of pursuing prosecution for criminal non-support of a child.

3.2.1.2.1.4. Providing a certified copy of the court order timely to the OAG upon request.

3.2.1.2.2. The County Customer Service unit shall take inquiries and receive information by, but not limited to, e-mail, letters, phone calls, facsimiles and walk-ins.

3.2.2. Resources as used in this Customer Service Unit Resources and Services section include, but are not limited to, personnel, office space, equipment, phones and phone lines.

3.2.3. Customer Service Unit Documentation

3.2.3.1. County shall follow OAG procedures relating to data integrity, set forth in Attachment D, when accepting changes to case information *i.e.*, procedures to properly identify the caller.

3.2.3.2. County shall perform the Customer Service Unit services using the following guidelines:

- 3.2.3.2.1. Respond to written inquiries within five (5) County business days,
- 3.2.3.2.2. take action on information received within three (3) County business days,
- 3.2.3.2.3. document case record of action or information received at time of receipt,
- 3.2.3.2.4. follow up to a telephone inquiry within three (3) County business days,
- 3.2.3.2.5. return phone calls within three (3) County business days,
- 3.2.3.2.6. see a customer the same day or schedule appointment within three (3) County business days of request.

3.2.3.3. County shall use OAG processes and procedures for forwarding misdirected inquiries between the County, and the OAG and the OAG's designated agent where necessary by providing the toll free number to the OAG's Call Center (800-252-8014).

3.2.3.4. The electronic files associated with customer service activity that the County may receive and process are:

- 3.2.3.4.1. Full Service and Registry Only Collections, technical document name: Interface Control Document 012 (ICD012).
- 3.2.3.4.2. Registry Only Disbursement Data, technical document name: Interface Control Document 013 (ICD013).
- 3.2.3.4.3. Full Service and Registry Only Collection Adjustments, technical document name Interface Control Document 015 (ICD015).
- 3.2.3.4.4. Registry Only Case Data from Local Registries, technical document name: Interface Control document 050 (ICD050).

3.2.4. The electronic file associated with customer service activity that the County may transmit is:

3.2.4.1. OAG Systems and Local Registries Customer Service Activities, technical document name: Interface Control Document 035 (ICD035).

3.2.5. In the event of a failed transmission, or if a file is unable to be processed, County shall correct the problem and retransmit within one (1) business day of notification by the OAG.

3.2.6. County shall record on its automated system all financial data available from the OAG required to support the accurate dissemination of payment record information contemplated by this Contract or the County shall access, as needed, an OAG/TXCSES payment history record, as available, from the OAG TXCSES Web application.

3.3. ACCESSING OAG SYSTEMS

3.3.1. County Responsibilities

3.3.1.1. Work with the OAG or its designated agent to acquire, when needed, (at no cost to the County) from the OAG or its designated agent one personal computer, including the necessary software, to access the OAG Systems. County will work with the OAG or its designated agent to obtain the database access required. County is responsible for connecting the hardware to its own County network and for the cost associated therewith.

- 3.3.1.2. County must make necessary programming changes to its own automated child support system to accomplish the local customer service activities in this Contract. If the County employs a Vendor for maintenance and changes to its automated child support system, County must coordinate efforts between the County Vendor and the OAG or its designated agent.
- 3.3.1.3. Should the County desire to retain their legacy case management system, whether in-house or vendor based, the County is required to maintain strict data synchronization with the OAG Systems. To accomplish this, the County must demonstrate sufficient resources and ability to receive and process into the County legacy system daily data updates from the OAG in ICD050 format.
- 3.3.1.4. County will be authorized to implement the data synchronization process upon completion of demonstrated ability and a documented system test.
- 3.3.1.5. Whether the County retains their legacy case management system or if data synchronization with the OAG Systems is not feasible the County shall enter all case/member information directly onto the designated OAG System unless agreed to otherwise in writing by the OAG Contract Manager.
- 3.3.1.6. The ICD050 computer file specifications and format will be made available to the County on the OAG child support portal. If these specifications change during the term of the Contract, the changes will be made available on the OAG child support portal and an e-mail notice of such availability will be sent to the County liaison. The County shall be responsible for implementing the changes to the electronic file specifications when and as required for OAG Systems processing, within a reasonable time frame.
- 3.3.1.7. To the extent necessary to fulfill its obligations under this Contract, County shall maintain, at no cost to the OAG, County hardware and software compatibility with the OAG Computer Systems and OAG file format needs, to include OAG software and OAG computer hardware and related equipment upgrades. OAG will provide County with as much notice as possible of intended OAG Computer Systems upgrades.
- 3.3.1.8. County is responsible for all the necessary phone lines. For those counties that do not have internet access the OAG will ensure that internet service is established for at least one personal computer. However, if the County is not covered by a local Internet Service Provider local telephone coverage area, then the County is responsible for any unavoidable long distance telephone charges that occur.

3.4. OAG Responsibilities

- 3.4.1. OAG will work with the County to make sure the County has one personal computer, including the necessary software, to access the OAG Systems. For those counties that do not have internet access, the OAG will ensure that internet service is established for at least one personal computer. However, if the County is not covered by a local Internet Service Provider local telephone coverage area, then the County is responsible for any unavoidable long distance telephone charges that occur.

4. REIMBURSEMENT

- 4.1. OAG shall monitor County OAG Systems State Case Registry and, if applicable, Local Customer Service activities (direct data entry or electronic file) and summarize for monthly reimbursement amounts.
- 4.2. OAG shall forward a Summary and Reimbursement Voucher for any particular month's activities to the County for review and approval by the 25th day of the following month.

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

4.3.1. County shall submit the invoice to:

Contract Manager, State Case Registry and Local Customer Service
Mail Code: 062
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

4.4. If County does not approve the Summary and Reimbursement Voucher, it shall return the voucher to the OAG within ten (10) County business days of receipt, detailing the basis of any disputed item, and include supporting documentation. The OAG shall review the returned voucher. If the dispute is resolved in the County's favor the OAG shall make payment as set forth in the preceding subsection. If the dispute is not resolved in the County's favor, the OAG shall make payment in accordance with the voucher originally sent to the County and forward a letter of explanation to the County.

4.4.1. OAG Rights Upon Loss of Funding

4.4.1.1. Legislative Appropriations

4.4.1.1.1. All obligations of the OAG are subject to the availability of legislative appropriations and, for federally funded procurements, to the availability of federal funds applicable to this procurement (see Provision of Funding by the United States, subsection below). 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 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 will not be considered to be in default or breach under this Contract, nor shall it be liable for any further payments ordinarily due under this Contract, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination. The OAG shall make best efforts to provide reasonable written advance notice to County of any such termination. In the event of such a termination, County shall, unless otherwise mutually agreed upon in writing, cease all work immediately upon the effective date of termination. OAG shall be liable for payments limited only to the portion of work the OAG authorized in writing and which the County has completed, delivered to the OAG, and which has been accepted by the OAG. All such work shall have been completed, per the Contract requirements, prior to the effective date of termination.

4.4.2. Provision of Funding by the United States

4.4.2.1. It is expressly understood that any and all of the OAG's obligations and liabilities hereunder are contingent upon the existence of a state plan for child support enforcement approved by the United States Department of Health and Human Services 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 such approval of the state plan or the availability of Federal Financial Participation should lapse or otherwise terminate, the OAG, in its discretion, may terminate this contract, either in whole or in part. In the event of such termination, the OAG will not be considered to be in default or breach under this contract, nor shall it be liable for any further payments ordinarily due under this contract, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination. The OAG shall make best efforts to provide reasonable written advance notice to Contractor of any such termination. In the event of such a termination, County shall, unless otherwise mutually agreed upon in writing, cease all work immediately upon the effective date of termination. OAG shall be liable for payments limited only to the portion of work the OAG authorized in writing and which the County has completed, delivered to the OAG, and which has been accepted by the OAG. All such work shall have been completed, per the Contract requirements, prior to the effective date of termination.

4.5. Reimbursement Rates

4.5.1. State Case Registry

4.5.1.1. The OAG shall be financially liable to the County for the federal share of the County's Contract associated cost. Federal share means the portion of the County's Contract associated 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 Contract is 66%. The County agrees that for the purposes of this Contract all of the County's Contract associated costs for any given calendar month is equal to the number of new and modified Registry Only Court Orders (together with all required data elements) provided to the OAG during the calendar month multiplied by a per new and modified Registry Only Court Order fee of \$12.81 plus the number of Registry Only Court Orders updated during the calendar month multiplied by a per Registry Only Court Order updated fee of \$4.07 per Registry Only Court Order updated. Thus: [(Calendar Month new and modified Registry Only Court Orders provided x \$12.81) + (Calendar Month Registry Only Court Orders updated x \$4.07)] x Federal Share = OAG Liability.

4.5.2. Local Customer Service

4.5.2.1. The OAG shall be financially liable to the County for the federal share of the County's Contract associated cost. Federal share means the portion of the County's Contract associated 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 Contract is 66%. The County agrees that for the purposes of this Contract all of the County's Contract associated costs for any given calendar month is equal to the number of inquiries on IV-D cases handled by County personnel during the calendar month, plus the number of inquiries on Registry Only cases (See Section 3.2.1 for the meaning of Registry Only cases) minus the Federal Disallowance Percentage, multiplied by a per inquiry fee of \$4.19 per inquiry. For purpose of reference only the Federal Disallowance Percentage for SFY 2011 annualized is 19%. Thus: (Calendar Month IV-D Inquiries Handled by County Personnel) + (Calendar Month Registry Only Inquiries Handled by County Personnel - Federal Disallowance Percentage) x (\$4.19) x (Federal Share) = OAG Liability.

4.6. Limitation of OAG Liability

- 4.6.1. The OAG shall be liable only for Contract associated costs incurred after commencement of this Contract and before termination of this Contract.
- 4.6.2. The OAG may decline to reimburse Allowable Costs which are submitted for reimbursement more than sixty (60) calendar days after the State Fiscal Year calendar quarter in which such costs are incurred.
- 4.6.3. 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 County agree has resulted in an overpayment to County, provided that such sums may be offset and deducted from any amount owing but unpaid to County.
- 4.6.4. The OAG shall not be liable for reimbursing the County if the County fails to comply with the State Case Registry Activities, the County Customer Service Unit Resources and Services, and/or the Customer Service Unit Documentation Sections above in accordance with the requirements of those sections.
- 4.6.5. The OAG shall not be liable for reimbursing the County for any activity currently eligible for reimbursement as of right without the necessity for a prior existing contract e.g. sheriff/processor fees. Nor shall the OAG be liable for reimbursing the County for any activities eligible for reimbursement under another contract or Cooperative Agreement with the OAG e.g. customer service related to cases in the same County's Integrated Child Support System ("ICSS") caseload, when the County has an ICSS contract with the OAG. Nor shall the OAG be liable for reimbursing the County for information correcting erroneous information previously provided by the County.
- 4.6.6. Notwithstanding any other provision of this Contract, the maximum liability of the OAG under this Contract is **Seven Hundred Dollars and No Cents (\$700.00)**.

4.7. Assignment of Claims

- 4.7.1. County hereby assigns to the OAG any claims for overcharges associated with this Contract under 15 U.S.C. §1, et seq., and Tex. Bus. & Comm. Code §15.01, et seq.

5. CONTRACT MANAGEMENT

5.1. Written Notice Delivery

- 5.1.1. Any notice required or permitted to be given under this Contract by one party to the other party shall be in writing and shall be addressed to the receiving party at the address hereinafter specified. 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.

5.1.1.1. County

The address of the County for all purposes under this Contract and for all notices hereunder shall be:

The Honorable Kim Nagypal (or his/her successor in office)
Tyler County District Clerk
100 W Bluff St Rm. 203
Woodville, TX 75979

5.1.1.2. OAG

The address of the OAG for all purposes under this Contract and for all notices hereunder shall be:

Alicia G. Key (or her successor in office)
Deputy Attorney General for Child Support
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

With copies to:

Joseph Fiore (or his successor in office)
Managing Attorney, Contracts Attorneys, Child Support Division
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

and

Allen Broussard (or his successor in office)
Manager, Government Contracts
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

5.2. Controlled Correspondence

5.2.1. After execution of this Contract, for a communication between the County and the OAG to be considered authoritative and binding it must be in writing and generated in accordance with procedures mutually agreed to by the County and the OAG. The OAG has procedures in place to number and track such communications as Controlled Correspondence. Any communication not generated in accordance with such procedures and not signed out by a designated position shall not be binding upon the parties and shall be of no effect. The OAG IV-D Director and the Contract Manager are designated as authorized signatories for all Controlled Correspondence with the County on behalf of the OAG. Unless otherwise notified by the County, the OAG shall consider the District Clerk or Local Registry's office, as the County signatory to this Contract, as authorized signatories for all Controlled Correspondence on behalf of the County. In the case of any inconsistency or conflict between such procedures and a Contract provision, the Contract provision shall control. Controlled Correspondence shall not be used to change pricing or alter the provisions of this Contract. Any such change requires a Contract amendment. Controlled Correspondence may be used to document interpretations of the provisions of this Contract.

5.3. Inspections, Monitoring and Audits

5.3.1. The OAG may monitor and/or conduct fiscal and/or program audits and/or investigations of the County's program performance at reasonable times. The OAG may at its option or at the request of County provide technical assistance to assist County in the operation of this program. County shall provide physical access without prior notice to all sites used for performance of service under this Contract to the OAG, United States Department of Health and Human Services, Comptroller General of the United States, and State Auditor of Texas. County shall grant to the OAG, the United States Department of Health and Human Services, Comptroller General of the United States, and State Auditor of Texas access, without prior notice, to all books, documents, and records of the County pertinent to this Contract. The County books, documents, and records may be inspected, monitored, evaluated, audited and copied. County shall cooperate fully with

the OAG, United States Department of Health and Human Services, Comptroller General of the United States, and State Auditor of Texas in the conduct of any audit and/or investigation including the providing of any requested books, documents, and records. County shall retain all financial records, supporting documents, statistical records, and any other records, documents, papers, logs, audit trails or books (collectively referred to as records) relating to the performances called for in this Contract. County shall retain all such records for a period of three (3) years after the expiration of the term of this Contract, or until the OAG or the United States are satisfied that all audit claim, negotiation, and litigation matters are resolved, whichever period is longer. Reports or other information relating to this program prepared by the County or at the request of the County shall be furnished to the OAG within ninety (90) days of availability. The requirements of this Subsection shall be included in all subcontracts.

5.4. Reimbursement of Audit Penalty

- 5.4.1. If funds are disallowed as a result of an audit finding contained in an audit (by County or County's independent auditor, 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) that County has failed to follow federal requirements for the IV-D program, then County agrees that the County shall refund to OAG the amount disallowed 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.

5.5. Remedies for Non-Performance

- 5.5.1. Failure of the County to perform the contracted for services as required by this Contract shall be considered unsatisfactory performance. Any finding of unsatisfactory performance shall be communicated to the County in writing by the OAG Contract Manager. If the County wants to dispute the finding, a written dispute must be received by the OAG Contract Manager no later than fifteen (15) calendar days from the date the County received the written finding of unsatisfactory performance. The written dispute must detail why the County believes the finding is erroneous and must contain all supporting documentation. The OAG Contract Manager will review the dispute submission to determine the validity of the original finding of unsatisfactory performance. The determination of the OAG Contract Manager shall be final and shall conclude the review process. The OAG Contract Manager's determination shall be communicated to the County in writing. If a written dispute of the original finding of unsatisfactory performance is not received by the OAG Contract Manager by the time set forth above, the finding of unsatisfactory performance shall be deemed validated and the County shall have waived its right to dispute the finding.
- 5.5.2. 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. Failure to provide an acceptable corrective action plan within the specified time period shall result in a withholding of payments due to County under this Contract until such time that an acceptable corrective action plan is provided.
- 5.5.3. If the County does not return to satisfactory status within four months of receiving notice that an unsatisfactory performance finding has been validated, OAG may withhold payments due to County under this Contract until the County is once again performing satisfactorily. If the unsatisfactory status persists for a total of six months after receiving notice of the validated unsatisfactory performance finding, OAG may terminate this Contract (in accordance with the Termination Section below) without payment to County for any costs incurred by County from the time that OAG commenced withholding payments due to County being in an unsatisfactory status. Where payments are to resume due to County having provided an acceptable corrective action plan or 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.

5.6. Training on OAG Systems

- 5.6.1. Any County staff performing functions under this Contract must be trained on OAG Systems. Classroom Training on OAG Systems will be scheduled upon request from the County, by the end of the quarter following such request. Classroom Training will be provided by OAG Regional Trainers at each of the OAG Regional Training Centers. County shall be responsible for any and all costs associated with this training, including, but not limited to, costs for travel, lodging, meals and per diem; provided, however that the OAG shall be responsible for the cost of training materials and equipment required to complete the training class. County is responsible for scheduling the training with the OAG and shall direct training requests to:

Larry Acevedo
Office of the Attorney General
Mail Code 053
PO Box 12017
Austin, TX 78711-2017
email address: CSD-TRN@texasattorneygeneral.gov

5.7. Assignment

- 5.7.1. County will not assign its rights under this Contract or delegate the performance of its duties under this Contract without prior written approval from the OAG.

5.8. Liaison

- 5.8.1. County and OAG each agree to maintain specifically identified liaison personnel for their mutual benefit during the term of the Contract. The liaison(s) named by County shall serve as the initial point(s) of contact for any inquiries made pursuant to this Contract by OAG and respond to any such inquiries by OAG. The liaison(s) named by OAG shall serve as the initial point(s) of contact for any inquiries made pursuant to this Contract by County and respond to any such inquiries by County. The liaison(s) shall be named in writing at the time of the execution of this Contract. Subsequent changes in liaison personnel shall be communicated by the respective parties in writing.

5.9. Subcontracting

- 5.9.1. It is contemplated by the parties hereto that County shall conduct the performances provided by this Contract substantially with its own resources and through the services of its own staff. In the event that County should determine that it is necessary or expedient to subcontract for any of the performances specified herein, County shall subcontract for such performances only after County has transmitted to the OAG a true copy of the subcontract County proposes to execute with a subcontractor and has obtained the OAG's written approval for subcontracting the subject performances in advance of executing a subcontract. County, in subcontracting for any performances specified herein, expressly understands and acknowledges that in entering into such subcontract(s), the OAG is in no manner liable to any subcontractor(s) of County. In no event shall this provision relieve County of the responsibility for ensuring that the performances rendered under all subcontracts comply with all terms of this Contract.

5.10. Dispute Resolution Process for County Breach of Contract Claim

- 5.10.1. 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.
- 5.10.2. County's claim for breach of this Contract 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 the County otherwise entitled to notice under this Contract. Compliance by the 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.
- 5.10.3. 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 immediate preceding subsection.
- 5.10.4. 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 Contract by the OAG nor any other conduct of any representative of the OAG relating to the Contract shall be considered a waiver of sovereign immunity to suit.
- 5.10.5. 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.
- 5.10.6. Neither the occurrence of an event nor the pendency of a claim constitutes grounds for the suspension of performance by the County, in whole or in part.

5.11. Reporting Fraud, Waste or Abuse

- 5.11.1. County 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:
 - 5.11.1.1. the Contract Manager
 - 5.11.1.2. the Deputy Director for Contract Operations, Child Support Division
 - 5.11.1.3. the Director, Child Support Division the Deputy Director, Child Support Division
 - 5.11.1.4. the OAG Ethics Advisor
 - 5.11.1.5. the OAG's Fraud, Waste and Abuse Prevention Program ("FWAPP") Hotline (866-552-7937) or the FWAPP E-mailbox (FWAPP@oag.state.tx.us)
 - 5.11.1.6. the State Auditor's Office hotline for fraud (1-800-892-8348).
- 5.11.2. The report of suspected misconduct shall include (if known):
 - 5.11.2.1. the specific suspected misconduct
 - 5.11.2.2. the names of the individual(s)/entity(ies) involved

- 5.11.2.3. the date(s)/location(s) of the alleged activity(ies)
- 5.11.2.4. the names and all available contact information (phone numbers, addresses) of possible witnesses or other individuals who may have relevant information; and
- 5.11.2.5. any documents which tend to support the allegations.

5.11.3. The words fraud, waste or abuse as used in this Section have the following meanings;

- 5.11.3.1. Fraud is the use of one's occupation for obtaining personal benefit (including benefit for family/friends) through the deliberate misuse or misapplication of resources or assets.
- 5.11.3.2. Waste is the extravagant careless or needless expenditure of funds or consumption of property that results from deficient practices, system controls, or decisions.
- 5.11.3.3. 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.

6. CONFIDENTIALITY AND SECURITY

6.1. Confidentiality and Security Provisions

6.1.1. General

- 6.1.1.1. 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.
- 6.1.1.2. 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.
- 6.1.1.3. This agreement requires County to retrieve data from the courts and other sources and create data within TXCSES or TXCSES Web.
- 6.1.1.4. 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. OAG rights and privileges applicable to OAG Data shall survive expiration or any termination of this Agreement, and shall be perpetual. 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.

- 6.1.1.5. 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.
- 6.1.1.6. 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 quarterly, OAG shall send County a list of TXCSES Web 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.
- 6.1.1.7. 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 an instance, 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.
- 6.1.1.8. All references to "Agreement Services" shall include activities within the scope of this Agreement.
- 6.1.1.9. 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 any requirements set forth in Attachment F, 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 the County has with anyone performing Agreement Services on County's behalf.
- 6.1.1.10. 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.

6.2. OAG Data Usage and Storage

- 6.2.1. 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 annually 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 A), 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 B) and the Child Support online Login Policy (Attachment C).

- 6.2.2. 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 F entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information".
- 6.2.3. 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.
 - 6.2.3.1. 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. This protection must include (where communication is through an external not-organization-controlled network [e.g. the Internet]) multifactor authentication that is compliant with NIST SP 800-63, Electronic authentication Guidance level 3 or 4, and shall be consistent with IRS Publication 1075 Section 4.7 Alternate Work Sites.

6.3. OAG Data Retention and Destruction, and Public Information Requests

- 6.3.1. 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 completed OAG-Child Support Division "Certificate of Destruction for Contractors and Vendors" (Attachment H; a copy of which is attached hereto and included herein).

- 6.3.2. 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.
- 6.3.3. 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 via fax any information requests to:

Public Information Coordinator
Office of the Attorney General
Fax (512) 494-8017

6.4. Security Incidents

6.4.1. Response to Security Incidents

- 6.4.1.1. County shall respond to detected security incidents. The term "security incident" means an occurrence or event where the confidentiality, integrity or availability 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:

- 6.4.1.1.1. Initial responders
- 6.4.1.1.2. Containment
- 6.4.1.1.3. Management Notification
- 6.4.1.1.4. Documentation of Response Actions
- 6.4.1.1.5. Expeditious confirmation of system integrity
- 6.4.1.1.6. Collection of audit trails and similar evidence
- 6.4.1.1.7. Cause analysis
- 6.4.1.1.8. Damage analysis and mitigation
- 6.4.1.1.9. Internal Reporting Responsibility
- 6.4.1.1.10. External Reporting Responsibility
- 6.4.1.1.11. OAG Contract Manager's and OAG CISO's name, phone number and email address.

- 6.4.2. Attachment G 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.

6.5. Notice

- 6.5.1. 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 Plan.
- 6.5.2. 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.
- 6.5.3. 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.
- 6.5.4. Whenever daily oral reports are provided, County shall provide, by close of business each Friday, an email report detailing the foregoing daily requirements.

6.6. Final Report

- 6.6.1. 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:
 - 6.6.1.1. a detailed explanation of the cause(s) of the security incident;
 - 6.6.1.2. 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
 - 6.6.1.3. 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 and a description of how the cure protects against the possibility of a recurrence.
- 6.6.2. If the cure has not been put in place by the time the report is submitted, County shall within thirty (30) calendar days after submission of the final report, provide a certification to OAG that states the date County implemented the cure and a description of how the cure protects against the possibility of a recurrence.
- 6.6.3. If County fails to provide a Final Report and Certification within forty-five (45) calendar days, or as otherwise agreed to, 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.

6.7. Independent Right to Investigate

- 6.7.1. 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.

6.8. Security Audit

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

6.8.1.1. 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:

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

6.8.1.1.2. 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; and

6.8.1.1.3. 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.

6.8.1.2. 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.

6.8.1.3. 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.

6.8.1.4. County shall supply to the OAG and the State of Texas any data or reports rendered or available in conjunction with any security audit of County or County's subcontractors, if such data or reports pertain, in whole or in part, to the Agreement Services. This obligation shall extend to include any report(s) or other data generated by any security audit conducted up to one (1) year after the date of termination or expiration of the Agreement.

6.9. Remedial Action

6.9.1. Remedies Not Exclusive and Injunctive Relief

6.9.1.1. 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.

- 6.9.1.2. 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.

6.10. Notice to Third Parties

6.10.1. 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. However, the notice method must comply with Section 521.053, Texas business and Commerce Code (as currently enacted or subsequently amended). Provided further that County must also comply with Section 521.053's "consumer reporting agency" notification requirements.

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

6.10.3. 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. However, the notice method must comply with Section 521.053, Texas business and Commerce Code (as currently enacted or subsequently amended). 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.

6.11. Commencement of Legal Action

6.11.1. 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.

7. AMENDMENT

7.1. This Contract shall not be amended or modified except by written amendment executed by duly authorized representatives of both parties. Any alterations, additions or deletions to the terms of this Contract which are required by changes in federal or state law are automatically incorporated into this Contract without written amendment to this Contract and shall be effective on the date designated by said federal or state law.

8. TERMINATION OF CONTRACT

8.1. Termination

8.1.1. Either party to this Contract shall have the right to either terminate this Contract in its entirety or in part. However, a County continuing to contract to provide Local Customer Service services must also continue to contract to provide State Case Registry services. The Contract, or portion of the Contract, may be terminated by the terminating party notifying the other party in writing of

such termination and the proposed date of the termination no later than thirty (30) calendar days prior to the effective date of such termination.

8.2. Survival of Terms

- 8.2.1. Termination of this Contract for any reason shall not release the parties from any liability or obligation set forth in this Contract that is expressly stated to survive any such termination or by its nature would be intended to be applicable following any such termination.

9. TERMS AND CONDITIONS

9.1. Federal Terms and Conditions

9.1.1. Compliance with Law, Policy and Procedure

- 9.1.1.1. County shall perform its obligations hereunder in such a manner that ensures its compliance with OAG, policy, processes and procedure. It shall also comply with all state and federal 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 carrying out the program of child support enforcement pursuant to Title IV, Part D of the federal Social Security Act of 1935 as amended; (2) providing services to the OAG as these laws, rules, regulations, requirements and guidelines currently exist and as they are amended throughout the term of this Contract. County understands and agrees that from time to time OAG may need to change its policy, processes or procedures and that such change shall not entitle County to any increased cost reimbursement under this Contract; provided, however, that County may exercise its right to terminate the Contract in accordance with the Termination Section above. OAG shall provide County e-mail notice of any change in OAG policy, processes or procedures.

9.1.2. Civil Rights

- 9.1.2.1. 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 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 provided by this Contract. 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.

9.1.3. Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion from Participation in Contracts Exceeding \$100,000.00.

- 9.1.3.1. County certifies by entering into this Contract, 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.
- 9.1.3.2. The certification requirement of this provision shall be included in all subcontracts that exceed \$100,000.

9.1.4. Environmental Protection (Contracts in Excess of \$100,000.00)

9.1.4.1. County shall be in compliance with all applicable standards, orders, or requirements issued under section 306 of the Clean Air Act (42 USC 1857(h)) Section 508 of the Clean Water Act (33 USC 1368) Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15). The requirements of this provision shall be included in all subcontracts that exceed \$100,000.

9.1.5. Certain Disclosures Concerning Lobbying [Contracts in excess of \$100,000]

9.1.5.1. Certain Counties 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 submit at the time of execution of this Contract a Certification Regarding Lobbying (Attachment E). 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.

9.1.5.2. The requirements of this provision shall be included in all subcontracts exceeding \$100,000.

9.2. News Releases or Pronouncements

9.2.1. News releases, advertisements, publications, declarations, and any other pronouncements pertaining to this Contract by County, using any means or media, must be approved in writing by the OAG prior to public dissemination.

9.3. Date Standard

9.3.1. Four-digit year elements will be used for the purposes of electronic data interchange in any recorded form. The year shall encompass a two digit century that precedes, and is contiguous with, a two digit year of century (e.g. 1999, 2000, etc.). Applications that require day and Month information will be coded in the following format: CCYYMMDD. Additional representations for week, hour, minute, and second, if required, will comply with the international standard ISO 8601: 1988, "Data elements and interchange formats--Information interchange--Representation of dates and times."

9.4. Headings

9.4.1. The headings for each section of this Contract are stated for convenience only and are not to be construed as limiting.

9.5. Agreement Relating to Debts or Delinquencies Owed to the State

9.5.1. As required by §2252.903, Government Code, the County agrees that any payments due under this Contract shall be directly applied towards eliminating any debt or delinquency including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support.

9.6. Certification Concerning Dealings with Public Servants

9.6.1. County, by signing this contract, 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.

9.7. Personnel Comportment

9.7.1. County and County subcontractor personnel and agents shall be courteous and professional in all communications during their performance of the requirements of this contract. 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 contract must have qualifications for the assigned position that equal or exceed those of the person being replaced.

9.8. Non-Waiver of Rights

9.8.1. Failure of a party to require performance by another party under this Contract 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 Contract 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 Contract will not be construed as a waiver of any continuing or succeeding breach. Should any provision of this Contract be invalid or unenforceable, the remainder of the provisions will remain in effect.

9.9. No Waiver of Sovereign Immunity

9.9.1. The parties expressly agree that no provision of this contract is in any way intended to constitute a waiver by the OAG or the State of Texas of any immunities from suit or from liability that the OAG or the State of Texas may have by operation of law.

9.10. Severability

9.10.1. If any provision of this contract is construed to be illegal or invalid, such construction will not affect the legality or validity of any of its other provisions. The illegal or invalid provision will be deemed severable and stricken from the contract as if it had never been incorporated herein, but all other provisions will continue in full force and effect.

9.11. Applicable Law and Venue

9.11.1. Applicable Law and Venue: County agrees that this Contract 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 Contract 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 Contract shall be brought in a court of competent jurisdiction in Tyler County. All payments under this Contract shall be due and payable in Travis County, Texas.

9.12. Entire Contract

9.12.1. This instrument constitutes the entire Contract between the parties hereto, and all oral or written contracts between the parties relating to the subject matter of this Contract that were made prior to the execution of this Contract have been reduced to writing and are contained herein.

9.13. Counterparts

9.13.1. This Contract 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.

9.14. Attachments

- 9.14.1. Attachment A: OAG Information Security Policy Manual
- 9.14.2. Attachment B: OAG Automated Computer System Access - Statement of Responsibility
- 9.14.3. Attachment C: Child Support Online Login Policy
- 9.14.4. Attachment D: Data Integrity Procedures Changes to Case Information
- 9.14.5. Attachment E: Certification Regarding Lobbying
- 9.14.6. Attachment F: IRS Publication 1075 (Rev. 8-2010)
- 9.14.7. Attachment G: Incident Response Plan
- 9.14.8. Attachment H: Certificate of Destruction for Contractors and Vendors

THIS CONTRACT IS HEREBY ACCEPTED

OFFICE OF THE ATTORNEY GENERAL

TYLER COUNTY

Alicia G. Key
Deputy Attorney General for Child Support

The Honorable Jacques Blanchette
County Judge, Tyler County



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 Donaho-Jaeger
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

Office of the Attorney General

- 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.¹

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.ⁱⁱ 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.ⁱⁱⁱ The state agency head or his or her designated representative(s) shall review and approve ownership of information resources and their associated responsibilities.^{iv} 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.^v

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.^{vi} 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.^{vii} 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.^{viii}

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.^{ix}

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.^x

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.^{xi}

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.^{xii}

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

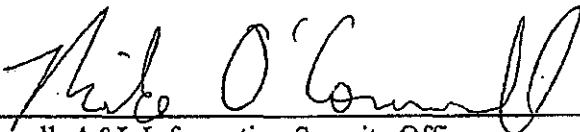
Notwithstanding any provisions to the contrary contained herein, waivers, exceptions and modifications to the information security policies and procedures may be authorized in writing at the discretion of the First Assistant Attorney General.

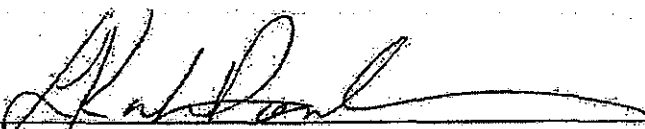
7. Document Acceptance and Release Notice


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 Donahoe-Jaeger, CSD Information Security Officer

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

8. References

-
- ⁱ Tex. Gov't Code § 2054.003(7).
- ⁱⁱ 1 TAC § 202.20.
- ⁱⁱⁱ 1 TAC § 202.1
- ^{iv} 1 TAC § 202.21.
- ^v 1 TAC § 202.21.
- ^{vi} 1 TAC § 202.21.
- ^{vii} 1 TAC § 202.27.
- ^{viii} *See generally*, 1 TAC Chapter 202.
- ^{ix} 1 TAC § 202.21.
- ^x 1 TAC § 202.1.
- ^{xi} 1 TAC § 202.26.
- ^{xii} 1 TAC § 202.25(6)(B).



ATTORNEY GENERAL OF TEXAS GREG ABBOTT

My Account Logout

Agreements

Statement

OFFICE OF THE ATTORNEY GENERAL - AUTOMATED COMPUTER SYSTEM ACCESS STATEMENT OF RESPONSIBILITY

General Information:

All information maintained in the files and records of the Child Support Division are privileged and confidential. The unauthorized use or release of the information can result in criminal prosecution and civil liability. Only authorized personnel may add, modify and/or delete information.

Statements:

I understand that the information concerning any person, customer or client that may come to my knowledge while using the computer system of the TXCSDU or TXCSES or any other OAG computer shall be held in strictest confidence and may not be disclosed, except as used exclusively for purposes directly connected with the administration of programs under Title IV-A, IV-D and IX of the federal Social Security Act and the OAG Confidentiality Policy and Procedures.

Notwithstanding the above, I understand that I may not disclose to any individual or agency any federal tax return or return information. I further understand that it is unlawful to offer or receive anything of value in exchange for federal tax return or return information. Such unauthorized disclosure or exchange is punishable by fine up to \$5,000, or imprisonment up to 5 years, or both, under Internal Revenue Code 7213 and 7215. Accessing federal tax information without a "need to know" is a federal misdemeanor punishable by not more than one year imprisonment, or a \$1,000 fine or both, plus costs of prosecution, under 26 U.S.C. Internal Revenue Code 7431 and 7432 and the user may be civilly liable for damages of not less than \$1,000 per violation, together with costs of prosecution under Section 7431 of the Internal Revenue Code.

I also understand that I may not release information to any committee or legislative body, federal, state, or local that identifies by name or address any such applicant or recipient of services, use of such information by a local government or component thereof for any other purpose, including but not limited to collecting a fee is prohibited.

I understand that I may not perform any work, review, update or otherwise act to obtain information upon my own, or any relatives, friends, or business associates child support case, regardless if the case is open or closed. My failure to comply with the OAG Confidentiality Policy will result in immediate termination of my computer access. I also understand that a violation will be reported to my supervisor or other appropriate personnel in my agency for disciplinary action, which may include termination and/or referral for prosecution.

In addition, if applicable, I understand that the computer password(s) I receive or devise is confidential, and must not be disclosed to anyone. I understand that it is my responsibility to safeguard such password(s) by not allowing it to be viewed by anyone. I understand that I am responsible for computer transactions performed through misuse of my password(s).

I agree I will not load unauthorized software, personal computer programs, shareware or freeware of any kind onto the OAG computer equipment without the express written approval of the Office of the Attorney General, Information Resource Manager, or designee, or the contract manager or designee. I understand that use of a password not issued or devised specifically for me is expressly prohibited and is a violation of state and federal law.


I also understand that 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 federal statutes may also be applicable.

I certify that I understand that any copyrighted material, including but not limited to 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.

By agreeing to this statement I certify that I:

- agree to abide by all written conditions imposed by the OAG regarding information security;
- understand my responsibilities as described above;
- have received, read and understand the OAG security information policy manual; and
- if applicable, I have read all applicable software licenses and agree to abide by all restrictions.

Home | Child Support Home | Download Adobe Reader™



ATTORNEY GENERAL OF TEXAS

GREG ABBOTT

My Account Logout

Agreements

Policy

WARNING

This system may contain U.S. Government Information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browning Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

When you register for the OAG Portal Service, we may ask you to give us certain identifying information ("Registration"), such as your name, address, and e-mail or the company's name and address and the company representative's name and e-mail address. This information will be used solely for Child Support (CD) purposes.

You agree to provide true, accurate, current, and complete information about yourself and your company. You also agree not to impersonate any person or entity, misrepresent any affiliation with another person, entity or association, use false headers or otherwise conceal your identity from the OAG for any purpose.

For your protection and the protection of our other members and Web site users, you agree that you will not share your Registration information (including passwords, User Names, and screen names) with any other person for the purpose of facilitating their access and unauthorized use of OAG Portal Services. You alone are responsible for all transactions initiated, messages posted, statements made, or acts or omissions that occur within any OAG Portal Service through the use of Registration information. Your failure to honor any portion of this agreement can result in termination of access to Portal Services.

Portal Tips | Accessibility | Privacy & Security Policy

Data Integrity Procedures Changes to Case Information

Before updating member/ case information, such as home address, phone number, etc., verify the caller's identity. Ask the caller for the following identifiers:

- Name
- Date of Birth
- Home address

If there is any doubt about the caller's identity after these identifier's have been obtained, ask for the children names and date of birth.

When pertinent information is unavailable on registry-only (RO) cases, county staff are prevented from verifying a caller's identity. Once all attempts to verify the caller's identity have been exhausted, instruct the caller to take one of the following actions in order to have the member/case information updated on TXCSESWeb:

- **Mail:**
 - a copy of a photo ID
 - information to be updated
 - proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.) to the county address

- **FAX:**
 - a photo ID
 - information to be updated
 - proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.) to the county FAX number

- **E-mail the information** to be updated with a scanned copy of the proof/verification information to be updated (ie., home address, SSN card, drivers license, etc.) to the county email address

- **In Person (District Clerk Office or Domestic Relations Office):**
 - a photo ID
 - information to be updated
 - proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.)

- **Visit the local child support office** that is assigned to work the RO case and provide:
 - a photo ID
 - information to be updated
 - proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.)



CERTIFICATION REGARDING LOBBYING
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES
FORM F

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 to 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 an 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 a 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 sub-awards at all tiers (including subcontracts, sub grants, and contracts under grants, loans, and cooperative agreements) and that all sub recipients 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

Title

Organization

The agency should include the Exhibit 7 language for either General Services or Technology Services, as appropriate and include the language below to the greatest extent possible, applicable to the specific situation.

CONTRACT LANGUAGE FOR GENERAL SERVICES

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 performed 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 by 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 and products will be given the same level of protection as required for the source material.
- (4) No work involving returns and 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.
- (7) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

- (1) 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 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 five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future 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 this 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 \$1,000.00 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 \$1,000.00 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. The penalties are prescribed by IRC Sections 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 so 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.

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

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 employees.
- (2) 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 will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be 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) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
- (7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (8) 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.
- (9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (10) (Include any additional safeguards that may be appropriate.)

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

**TYLER COUNTY
INCIDENT RESPONSE PLAN**

Adopted _____, 2012

Overview..... 3
Incident Response Team..... 3
Incident Response Team Roles and Responsibilities..... 4
Incident Contact List..... 5
 OAG Contact Information 5
 County Contact Information 5
ATTACHMENTS
Incident Identification..... 6
Incident Survey 7
Incident Containment..... 8
Incident Eradication 9

Tyler County Incident Response Plan

Overview

Pursuant to Contract #13-C0088, § 6.4.1.1, this Incident Response Plan is designed to provide a general guidance to county staff, both technical and managerial, to:

- enable quick and efficient recovery in the event of security incidents which may threaten the confidentiality of OAG Data;
- respond in a systematic manner to incidents and carry out all necessary steps to handle an incident;
- prevent or minimize disruption of mission-critical services; and,
- minimize loss or theft of confidential data.

The plan identifies and describes the roles and responsibilities of the Incident Response Team and outlines steps to take upon discovery of unauthorized access to confidential data. The Incident Response Team is responsible for putting the Plan into action.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to any threat to confidential data. The Team's mission is to prevent a serious loss of information assets or public confidence by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Team is responsible for investigating suspected security incidents in a timely manner and reporting findings to management and the appropriate authorities as appropriate.

Incident Response Team Roles and Responsibilities

Position	Roles and Responsibilities
Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> • Immediately report incident directly to OAG CISO and OAG Contract Manager • Determine nature and scope of the incident • Contact members of the Incident Response Team • Determine which Team members play an active role in the investigation • Escalate to executive management as appropriate • Contact other departments as appropriate • Monitor and report progress of investigation to OAG CISO • Ensure evidence gathering and preservation is appropriate • Prepare and provide a written summary of the incident and corrective action taken to OAG CISO
Information Technology Operations Center	<ul style="list-style-type: none"> • Central point of contact for all computer incidents • Notify CISO to activate Incident Response Team • Complete Incident Identification form (Attachment One) and Incident Survey (Attachment Two) and forward to County CISO
Information Privacy Office	<ul style="list-style-type: none"> • Document the types of personal information that may have been breached • Provide guidance throughout the investigation on issues relating to privacy of customer and employee personal information • Assist in developing appropriate communication to impacted parties • Assess the need to change privacy policies, procedures and/or practices as a result of the breach
Network Architecture	<ul style="list-style-type: none"> • Analyze network traffic for signs of external attack • Run tracing tool and event loggers • Look for signs of firewall breach • Contact external internet service provider for assistance as appropriate • Take necessary action to block traffic from suspected intruder • Complete Incident Containment Forms (Attachment Three), as appropriate, and forward to County CISO
Operating Systems Architecture	<ul style="list-style-type: none"> • Ensure all service packs and patches are current on mission-critical computers • Ensure backups are in place for all critical systems • Examine system logs of critical systems for unusual activity • Complete Incident Containment Forms (Attachment Three), as appropriate, and forward to County CISO
Business Applications	<ul style="list-style-type: none"> • Monitor business applications and services for signs of attack • Review audit logs of mission-critical servers for signs of suspicious activity • Contact the Information Technology Operations Center with any information relating to a suspected breach • Collect pertinent information regarding the incident at the request of the CISO
Internal Auditing	<ul style="list-style-type: none"> • Review systems to ensure compliance with information security policy and controls • Perform appropriate audit test work to ensure mission-critical systems are current with service packs and patches • Report any system control gaps to management for corrective action • Complete Incident Eradication Form (Attachment Four) and forward to County CISO

Incident Contact List

OAG Contact Information

Position	Name	Phone Number	Email address
OAG Chief of Information Security Officer	Willie Harvey	512-936-1320	willie.harvey@texasattorneygeneral.gov
OAG Contract Manager	Allen Broussard	512-460-6373	allen.broussard@texasattorneygeneral.gov

County Contact Information

Position	Name	Phone Number	Email address
Chief of Information Security Officer			
County Contract Manager			
Information Technology Operations Center			
Information Privacy Office			
Network Architecture			
Operating Systems Architecture			
Business Applications			
Internal Auditing			

Incident Identification

Date Updated: _____

General Information

Incident Detector's Information:

Name: _____	Date and Time Detected: _____
Title: _____	Location Incident Detected From: _____
Phone: _____	_____
Email: _____	_____
Detector's Signature: _____	Date Signed: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Malicious Code
- Unauthorized Use
- Unauthorized Access
- Espionage
- Other _____
- Probe
- Hoax

Incident Location: _____

Site: _____

Site Point Of Contact: _____

Phone: _____

Email: _____

How was the Intellectual Property Detected:

Additional Information:

Incident Survey

Date Updated: _____

Location(s) of affected systems: _____

Date and time incident handlers arrived at site: _____

Describe affected information system(s): _____

Is the affected system connected to a network? YES NO

Is the affected system connected to a modem? YES NO

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etc.):

Incident Containment

Date Updated: _____

Isolate Affected Systems:

CISO approved removal from network? YES NO

If YES, date and time systems were removed: _____

If NO, state reason: _____

Backup Affected Systems:

Successful backup for all systems? YES NO

Name of person(s) performing backup: _____

Date and time backups started: _____

Date and time backups complete: _____

Incident Eradication

Date Updated: _____

Name of person(s) performing forensics on systems:

Was the vulnerability identified: YES NO

Describe: _____

Office of the Attorney General – Child Support Division
 Certificate of Destruction for Contractors and Vendors

ATTACHMENT H

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The OAG tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Contact Name	Title	Company Name and Address	Phone

You may attach an inventory of the media if needed for bulk media disposition or destruction.

Media Type		Media Title / Document Name	
<input type="checkbox"/> HARD COPY	<input type="checkbox"/> ELECTRONIC		
Media Description (Paper, Microfilm, Computer Media, Tapes, etc.)			
Dates of Records			
Document / Record Tracking Number	OAG Item Number	Make / Model	Serial Number

Item Sanitization	<input type="checkbox"/> CLEAR	Who Completed?	<input type="checkbox"/> Who Verified?
	<input type="checkbox"/> PURGE	Phone	Phone
	<input type="checkbox"/> DESTROY	DATE Completed	

Sanitization Method and/or Product Used →

Final Disposition of Media	<input type="checkbox"/> Reused Internally	<input type="checkbox"/> Destruction / Disposal
	<input type="checkbox"/> Reused Externally	<input type="checkbox"/> Returned to Manufacturer
	<input type="checkbox"/> Other:	

Comments:

If any OAG Data is retained, indicate the type of storage media, physical locations(s), and any planned destruction date.

Description of OAG Data Retained and Retention Requirements:

Proposed method of destruction for OAG approval:	Type of storage media?	
	Physical location?	
	Planned destruction date?	

Within five (5) days of destruction or purging, provide the OAG with a signed statement containing the date of clearing, purging or destruction, description of OAG data cleared, purged or destroyed and the method(s) used.

Authorized approval has been received for the destruction of media identified above and has met all OAG Records Retention Schedule requirements including state, federal and/or internal audit requirements and is not pending any open records requests.

Records Destroyed by:		Records Destruction Verified by:	
Signature	Date	Signature	Date

Be sure to enter name and contact info for who completed the data destruction and who verified data destruction in the fields above.

Send the signed Certificate of Destruction to:
 OAG: Child Support Division, Information Security Office, PO Box 12017, Austin, TX 78711-2017

INSTRUCTIONS FOR CERTIFICATE OF DESTRUCTION

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The OAG tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

IRS Publication 1075 directs us to the FISMA requirements and NIST guidelines for sanitization and disposition of media used for federal tax information (FTI). These guidelines are also required for sensitive or confidential information that may include personally identifiable information (PII) or protected health information (PHI). NIST 800-88, Appendix A contains a matrix of media with minimum recommended sanitization techniques for clearing, purging, or destroying various media types. This appendix is to be used with the decision flow chart provided in NIST 800-88, Section 5.

There are two primary types of media in common use:

- **Hard Copy.** Hard copy media is physical representations of information. Paper printouts, printer and facsimile ribbons, drums, and platens are all examples of hard copy media.
- **Electronic (or soft copy).** Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in NIST SP 800-88, Appendix A.

1. For media being reused within your organization, use the **CLEAR** procedure for the appropriate type of media. Then validate the media is cleared and document the media status and disposition.
2. For media to be reused outside your organization or if leaving your organization for any reason, use the **PURGE** procedure for the appropriate type of media. Then validate the media is purged and document the media status and disposition. Note that some **PURGE** techniques such as degaussing will typically render the media (such as a hard drive) permanently unusable.
3. For media that will not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.
4. For media that has been damaged (i.e. crashed drive) and can not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.
5. If immediate purging of all data storage components is not possible, data remaining in any storage component will be protected to prevent unauthorized disclosures. Within twenty (20) business days of contract expiration or termination, provide OAG with a signed statement detailing the nature of OAG data retained type of storage media, physical location, planned destruction date, and the proposed methods of destruction for OAG approval.
6. Send the signed Certificate of Destruction to:

OAG: Child Support Division
Information Security Office
PO Box 12017
Austin, TX 78711-2017

FAX to: 512-460-6070

or send as an email attachment to:

Willie.Harvey@cs.oag.state.tx.us

Final Distribution of Certificate	Original to:	Willie Harvey, Information Security Officer 512-460-6764
	Copy to:	1. Your Company Records Management Liaison - or - Information Security Officer 2. CSD Contract Manager

RESOLUTION

State of Texas §
County of Tyler §

WHEREAS, the Tyler County Commissioner's Court finds it in the best interest of the citizens of Tyler County, that the 'Software for Car Computers' Project be operated for the FY 2012 – 2013; and

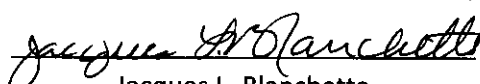
WHEREAS, the Tyler County Commissioner's Court agrees that in the event of loss or misuse of the Criminal Justice Division funds, the Tyler County Commissioner's Court assures that the funds will be returned to the Criminal Justice Division in full.

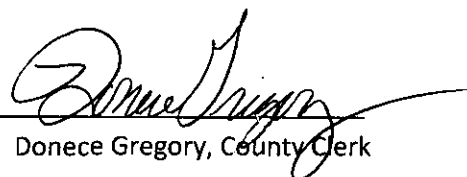
WHEREAS, the Tyler County Commissioner's Court designates the County Judge, as the grantee's authorized official. The authorized official is given the power to apply for, accept, reject, alter or terminate the grant on behalf of the applicant agency.

NOW THEREFORE, BE IT RESOLVED that the Tyler County Commissioner's Court approves submission of the grant application for the 'Software for Car Computers' Project to the Office of the Governor, Criminal Justice Division.

Passed and Approved by the Tyler County Commissioner's Court this 13th
of July, 2012.

Grant Number: 2590901


Jacques L. Blanchette
County Judge

ATTEST: 
Donece Gregory, County Clerk

**COMMUNICATIONS SITE AGREEMENT
BETWEEN COUNTY OF TYLER, TEXAS AND TEXAS FOREST SERVICE**

This Communications Site Agreement (the "Site Agreement"), entered into as of the 13th day of July, 2012 by and between the County of Tyler "County." ("Site Owner" or "Lessor") having an address at 100 West Bluff, Room 102, Woodville, Texas, 75979, and Texas Forest Service, a member of The Texas A&M University System, an agency of the state of Texas, "TFS" (Site User" or "Lessee") having an address at 301 Tarrow, Suite 419, College Station, Texas 77840. TFS and County are collectively called "the Parties."

In consideration of the mutual promises, conditions, covenants and considerations passing between the Parties hereto, it is understood and agreed by and between the Parties to this Site Agreement as follows:

Site Agreement is for tower and/or antenna and/or shelter and/or antenna space, including any wires, generator(s), equipment, etc. necessary to carry out Lessee's operation of the radio tower ("Tower Equipment") as listed in Exhibit "A" on Doucette site located in Tyler County County, Texas. Latitude: 30-50-08.90 Longitude: 094-25-52.20 together with access thereto ("Site"). Lessee is responsible for installing and maintaining Lessee's Tower Equipment at Lessee's expense.

1. **TERMS:** The Term of this Site Agreement shall be for a period of 5 years commencing on the 13th day of July, 2012, and terminating on the 13th day of July, 2017.
2. **CONSIDERATION:** The consideration for this Site Agreement is the sum of (\$1.00) per year.
3. **TITLE:** Lessee shall have no right, title or interest in the Site except the non-exclusive use thereof as expressly set forth in this Site Agreement. Lessee shall retain ownership of and title to all equipment and structures Lessee installs on the Site, even though such equipment and structures may be permanently affixed to the real property.
4. **ELECTRICITY:** Site Owner will provide electricity at the Site for the benefit of Lessee.

Lessee shall have the right to use the existing emergency stand-by generator(s) at the Site, if available; however Site Owner makes no representations or warranties as to the fitness of such generator(s) for Lessee's requirements.

5. **PERMITS, LICENSES AND REGULATIONS:** Lessee agrees and understands that it is Lessee's responsibility to abide by all federal, state, and local rules and regulations pertaining to Lessee's operation at the Site and to Lessee's equipment; including without limitations, those pertaining to the installation, maintenance, height, location, use, operation, and removal of Lessee's equipment, antenna systems, and other alterations or improvements authorized herein. Lessee hereby represents that Lessee has obtained the necessary licenses and permits required to use said Site, or that Lessee will obtain said licenses or permits, at Lessee's own expense, prior to any such use. Upon Lessee's request, Site Owner will provide Lessee a copy of the Antenna Structure Registration, if any, as provided to the Site Owner by the FCC.
6. **USE:** It is expressly agreed by Lessee that: (1) while using the Site, Lessee shall be responsible for proper operation and compliance with Federal Communication Commission ("FCC") rules; (2) if Site Owner is providing the tower to Lessee, Lessee hereby consents to the execution of agreements between Site Owner and other parties eligible to share the Site, whereby such parties may utilize and share said Site with Lessee; and (3) Lessee represents that it has independently ascertained that the Site is adequate and proper for Lessee's intended use and has entered into this Site Agreement based solely upon said independent investigation, and not by any representation by Site Owner.

If the Site Owner is providing the tower to Lessee, Lessee will not increase the size of its Tower Equipment or alter the wind load or structural impact of its equipment upon the tower, without the prior written consent of Lessor.

If Lessee is providing its own tower, Lessee has the right to construct, reconstruct and maintain a radio tower, with all necessary concrete foundations, footings, guy wires, shelters for the protection of the equipment necessary for the operation of the radio tower and any other structures necessary for the installation, operation and maintenance of the radio tower, in, upon and across the Site.

7. **COVERAGE AND INTERFERENCE:** Site Owner makes no representations concerning the distance at which useable radio signals may be transmitted and received from the Site or location thereof. Lessee is hereby notified that the Site is subject to degradation of performance from, but not limited to, natural and man-made phenomena such as so-called "skip" interference, power line and ignition noise, intermodulation, co-channel interference, and interference from users of the same or other radio frequencies.

Lessee shall be responsible for taking such reasonable steps as may be necessary to prevent any spurious radiation or objectionable interference with the broadcasting or transmission facilities of Site Owner or other users on the Site, if any, caused by Lessee. The determination of what is reasonable shall be within the sole discretion of Site Owner. If Lessee has not taken corrective measures within three business days after Site Owner notifies Lessee that Lessee's equipment is causing objectionable interference, then Site Owner may, in addition to its other rights or remedies, at its discretion:

- (1) disconnect power to Lessee's equipment and/or
- (2) terminate this Site Agreement by giving Lessee written notice.

Site Owner or its designated representatives shall have the sole right, initially and during the term of this Site Agreement, to:

- (a) determine the location of the equipment on the Site, and
- (b) require Lessee to take whatever action is necessary to eliminate objectionable interference by Lessee's equipment with devices approved by Site Owner.

Nothing contained in this Site Agreement shall be deemed to entitle Lessee to the exclusive possession of any vertical span of space on the Site, it being the intention of the Parties that the vertical span of space may be used by others at the direction of the Site Owner provided no objectionable interference is caused to Lessee's radio transmission activity. It is understood and agreed that Site Owner intends to and shall have the right to accommodate other transmitters and/or receivers at the Site, and in that connection it is understood and agreed that Site Owner shall have the right at any time during the term of this Site Agreement to locate the antenna or other equipment of other users within the same vertical space on the Site as Lessee may occupy, including the right to require the multiplexing or the transmission of other user(s) provided no objectionable interference is caused to Lessee's transmission activities thereby and, provided, further, that Lessee is not put to any cost in connection therewith. For purposes of this Site Agreement, objectionable interference shall be deemed to exist if:

- (1) a determination to that effect is made by an authorized representative of the FCC, or
- (2) a condition exists which constitutes interference within the meaning of the provisions of the Rules and Regulations of the FCC at the time in effect, or
- (3) there is a material impairment of sound, picture, data or other transmission in any material portion of the protected service area of such activity as such area is or may be defined by the FCC at any hour during the period of operation of such activity, as compared with that which would be obtained if no other users were transmitting from the Site or had any equipment at the Site, or
- (4) a user is prevented from using or having access to its equipment at reasonable and usual times to an extent to which interferes to a material degree with the operation and maintenance thereof, it being understood that a reasonable temporary interference which does not materially interfere with the operation or maintenance of said equipment and which is occasioned by the installation of the new equipment by another user, or by repairs to or maintenance of existing equipment of another user shall not be considered objectionable interference.

If appropriate to maintain safe or efficient operation of the Site, Lessee shall be required to participate in any transmitter and receiver combining and multicoupling systems operating from one or more antennas installed by Site Owner.

8. LESSEE'S MAINTENANCE AND REMOVAL OF EQUIPMENT AND COAXIAL CABLES:

Lessee shall install only the equipment, (including antenna and transmission line) which the Site Owner has approved in writing. The Lessee agrees that the installation will be done in a neat, professional manner and in compliance with all applicable laws and regulations. All costs (including repair of damages caused thereby to Lessee's equipment) will be the responsibility of the Lessee. If Lessee wants to add any additional equipment, other than Lessee's equipment referenced herein, Lessee cannot install such additional equipment until the parties execute a written amendment to this Site Agreement, authorizing the additional equipment.

Lessee shall properly ground all antenna equipment at the uppermost location of its equipment on the tower and properly ground its coaxial cable at the base of the tower, or at locations identified by the Site Owner.

Site Owner retains the right to paint all coaxial cables attached to the tower, including Lessee's coaxial cable, as necessary, in order to prevent "black leg".

9. INSPECTION AND ACCESS: Site Owner will provide Lessee unlimited ingress and egress to the Site for the purposes of constructing, reconstructing, operating, maintaining, inspecting, using, replacing, repairing, moving, removing, etc. the Tower Equipment (including any Lessee radio tower, footings, supporting foundations, guy wires, equipment, shelters and any and all necessary appurtenances thereto) and for complying with any reasonable request for inspection by representatives of the FCC. Lessee shall have access only to its own equipment and under no circumstances will Lessee gain access to other equipment located at the Site or allow anyone else access to equipment other than its own.

10. COORDINATION OF INSTALLATION, REPAIR AND MAINTENANCE: In the event of the need for installation, repair or maintenance of the Site Owner's tower, equipment building or other common facility, Site Owner agrees to coordinate such activities in such a manner as to minimize any downtime that may be caused to Lessee's operations. Lessee agrees to reduce or shut down the power of its transmitter if necessary at a coordinated time so that such installation, repair or maintenance may take place.

11. FAILURES AND MAINTENANCE: Lessee is hereby notified and understands that the Site will not provide communications 100% of the time and it will, by its very nature, fail and require maintenance from time to time without notice. Lessee has taken such facts into consideration prior to the execution of this Site Agreement, and such failures shall not constitute nonperformance or negligence on the part of the Site Owner. The Site Owner is not liable or responsible for interruptions or termination of service caused by strikes, lockouts, governmental acts, acts of God or other conditions beyond its control. Any such interruption or termination of service shall not be considered as a breach of this Site Agreement by Site Owner. The Lessee at its own expense shall be totally responsible for any and all maintenance of its equipment due to lightning, power line surges, ground faults, excessive voltage, or any other causes beyond the control of Site Owner.

12. TERMINATION OF LESSOR'S RIGHTS TO SITE: In the event that any state, local or federal government agency causes the Site and/or its location to become unavailable, or Site Owner's ground lease (if any) is terminated for any reason or Site Owner transfers the real property to another, Site Owner shall have the right to terminate this Site Agreement without liability to Lessee.

The Site Owner must notify Lessee within ten (10) calendar days of the occurrence of either of the following; however, Site Owner must also notify Lessee as soon as possible if either of the following becomes likely to occur: 1) the sale of the real property on which the Site is located; or 2) the termination of the Site Owner's ground lease or other authority to lease the real property on which the Site is located, if applicable.

13. **INSURANCE:** Site Owner provides no insurance on the Site or on Lessee's Tower Equipment or personnel.
14. **GENERAL PROVISIONS:** The undersigned certifies that he has read and understands all of the terms and conditions of this Site Agreement, and each party acknowledges receipt of a true copy hereof at the time of execution.
15. **CONTACTS AND COMPLAINTS:** Any contacts or notice required under this Site Agreement between the Parties shall be submitted in writing to the other party to the contact person and address listed below. If either party wants to change the contact person or address, the party shall provide reasonable written notice of the change to the contact person and address listed below.

In addition to other remedies contained in this Site Agreement, the Parties may direct their written complaints, as well as any contract claim, to the following office:

Texas Forest Service

ATTN: Carl Bridges @ 9e6-639-8140
Email: cbridges@tfs.tamu.edu
301 Tarrow, Suite 419
College Station, Texas 77840

Tyler County

ATTN: County Judge
Facsimile: (409) 331-0028
100 West Bluff, Room 102
Woodville, Texas 75979

16. **AUDIT CLAUSE:** The State Auditor may conduct an audit or investigation of any entity receiving funds from the State directly under this Site Agreement or indirectly through a subcontract under this Site Agreement. Acceptance of funds directly under this Site Agreement or indirectly through a subcontract under this Site Agreement acts as acceptance of the authority of the State Auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. Under the direction of the legislative audit committee, an entity that is the subject of an audit or investigation by the State Auditor must provide the State Auditor with access to any information the State Auditor considers relevant to the investigation or audit.
17. **GOVERNING LAW** - This Site Agreement shall be governed by the substantive and procedural laws of the State of Texas. The conflicts of law principles and rules of any other jurisdiction shall not apply.
18. **FORCE MAJEURE** - Except as otherwise provided, neither Site Owner, nor Lessee shall be liable to the other for any delay in performance of, or failure to perform, any obligation contained herein caused by force majeure, provided the party seeking to be excused has prudently and promptly acted to take any and all reasonable corrective measures that are within such party's control. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been corrected.

Force majeure is defined as those causes beyond the control of the party required to perform that are generally recognized under Texas law as a force majeure event, such as acts of God, acts of war, epidemic and court orders. The party claiming a force majeure event shall immediately upon discovery notify the other party in writing of any delays or failure to perform.

19. **SEVERABILITY** - If one or more provisions of this Site Agreement, or the application of any provision to any party or circumstance, is held invalid, unenforceable, or illegal in any respect by a final

order/judgment of the State Office of Administrative Hearings or a court of competent jurisdiction, the remainder of this Site Agreement and the application of the provision to other parties or circumstances will remain valid and in full force and effect.

20. **SURVIVAL** - Any provisions of this Site Agreement that impose continuing obligations on the Parties including, but not limited to the following, will survive the expiration or termination of this Site Agreement for any reason:
 - a. Audit rights and
 - b. Any other provisions of this Site Agreement that impose continuing obligations on either of the Parties or that govern the rights and limitations of either of the Parties after the expiration or termination of this Site Agreement.
21. **NON-WAIVER OF DEFAULTS** - Any failure of either party, at any time, to enforce or require the strict keeping and performance of any provision of this Site Agreement will not constitute a waiver of such provision, and will not affect or impair same or the right of either party at any time to avail itself of same.
22. **NO LIABILITY FOR EMPLOYEES AND OFFICERS** - Each party to this Site Agreement shall have no liability whatsoever for the actions or omissions of an individual employed by either party, regardless of where the individual's actions or omissions occurred. Each party is solely responsible for the actions and/or omissions of its employees, officers and agents; however, such responsibility is only to the extent required by Texas law. Where injury or property damage result from the joint or concurring negligence of the Parties, liability, if any, shall be shared by each party in accordance with the applicable laws of the State of Texas, subject to all defenses, including governmental immunity. These provisions are solely for the benefit of the Parties hereto and not for the benefit of any person or entity not a party hereto; nor shall any provision hereof be deemed a waiver of any defenses available by law.
23. **LEGISLATIVE ACTION** - Each party's authority is subject to the actions of the Texas Legislature and the United States Congress. If either party and/or the subject matter of this Site Agreement become subject to a legislative or regulatory change or the revocation of statutory or regulatory authority that would render the services and/or goods to be provided under this Site Agreement impossible, unnecessary, void or substantially amended or that would terminate the appropriations for this Site Agreement or the Site, either party may immediately terminate this Site Agreement without penalty to, or any liability whatsoever on the part of such party, the State of Texas and the United States. This contract does not grant Lessee a vested property right.
24. **TERMINATION BY DEFAULT** - In the event that either party fails to carry out or comply with any of the requirements of this Site Agreement, the other party may notify the failing party of such failure or default in writing and demand that the failure or default be remedied within ten (10) days. In the event that the failing party fails to remedy such failure or default within the ten (10) day period, the other party will have the right to cancel this Site Agreement upon ten (10) days written notice.
25. **TERMINATION FOR CONVENIENCE** -
Either party, without cause, may terminate this Site Agreement without penalty by giving thirty (30) days written notice of such termination to the other party.
26. **TERMINATION LIABILITY (FOR TERMINATION FOR CONVENIENCE)** - In no event will termination for convenience by either party give rise to any liability whatsoever on the part of the terminating party. However, if the Lessee is required by this Site Agreement to pay for use of the Site, Lessee is obligated to pay Site Owner the pro rata amount of compensation owed for the number of days on which Lessee used the Site during the term at issue. The phrase "used the Site" includes any days on which Lessee kept any of its equipment on the Site
27. **NO JOINT ENTERPRISE** - Lessee is associated with Site Owner only for the purposes and to the extent set forth herein, and with respect to the provision of the Site or the performance of any services herein, Site Owner is and shall be an independent contractor and shall have the sole right to supervise, manage,

operate, control, and direct the performance of the details incident to its duties hereunder. Nothing contained herein shall be deemed or construed to create a partnership or joint venture, to create the relationships of an employer-employee or principal-agent, or to otherwise create any liability for either party whatsoever with respect to the indebtedness, liabilities, and obligations of the other party.

28. **ASSIGNMENT BY EITHER PARTY** – Neither party is authorized to assign or transfer any interest in this Site Agreement without the express, prior written consent of the other party.
29. **SUCCESSORS** - This Site Agreement shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors, heirs, administrators, personal representatives, legal representatives and permitted assigns.
30. **REMOVAL OF LESSEE'S EQUIPMENT** – Lessee is required to remove all of Lessee's Tower Equipment (including any radio tower, footings, supporting foundations, guy wires, equipment, shelters and any and all necessary appurtenances thereto) at Lessee's sole risk and expense, within a reasonable amount of time, not to exceed 120 days, after the termination of this Site Agreement. Lessee is also required to remove any debris associated with the removal of the Tower Equipment.
31. **CONTRACT AMENDMENTS** - No modification or amendment to this Site Agreement will become valid unless in writing and signed by both Parties. All correspondence regarding modifications or amendments to this Site Agreement must be forwarded to Tyler County for prior review and approval. Only the County Judge will be authorized to sign changes or amendments for Tyler County and only with approval of the Tyler County Commissioners Court.
32. **INTERPRETATION AGAINST THE DRAFTER** - Regardless of which party drafted the Site Agreement or the language at issue, any ambiguities in the Site Agreement or the language at issue will not be interpreted against the drafting party.
33. **NON-INCORPORATION CLAUSE** - This Site Agreement embodies the entire agreement between the Parties regarding the Site and Tower Equipment, and there have been and are no oral or written covenants, agreements, understandings, representations, warranties or restrictions between the Parties regarding the Site and Tower Equipment described in this Site Agreement other than those specifically set forth herein.
34. **MULTIPLE CONTRACTS** - This Site Agreement may be executed in a number of identical counterparts, each of which shall be deemed an original for all purposes. In making proof of this Site Agreement, it shall not be necessary to produce or account for more than one such counterpart.
35. **HEADINGS** - The headings, captions and arrangements used in this Site Agreement are, unless specified otherwise, for convenience only and shall not be deemed to limit, amplify or modify the terms of this Site Agreement, nor to affect the meaning thereof.
36. **AUTHORITY**: Any individual signing this Site Agreement on behalf of an entity represents and warrants that he has full authority to do so.

This Site Agreement shall be binding upon the respective successors, assigns and personal representatives of the parties.

SITE OWNER:

TYLER COUNTY

(Signature)

Jacques L. Blanchette
Jacques L. Blanchette, County Judge

7-13-12 (Date)

LESSEE:

TEXAS FOREST SERVICE

(Signature)

_____ (Date)

EXHIBIT A

- (a) This agreement provides for one antenna mounted at highest level below the top of the tower where existing antennas are mounted so that there is separation and no cross interference with the existing radio systems performance. The amateur radio antenna is to be mounted at or below that same level so that it does not interfere with existing or Lessee's radio performance.
- (b) Floor space within Site Owner's existing equipment shelter, sufficient to accommodate the equipment of Lessee without encroaching on space utilized and occupies by existing equipment in the shelter.
- (c) Lessee agrees to install an air conditioning unit in the shelter purchased and installed at Lessee's expense that is sufficient to maintain an appropriate inside temperature of the building suitable for the safe and efficient operation of both Site Owner's and Lessee's equipment housed in the building Site Owner will provide, at Site Owner's expense, electrical service for the operation of this air conditioning equipment the same as with other equipment housed in the building.
- (d) In addition to other terms and agreements provided for this in this document, Lessee agrees, at the time of the installation of Lessee's equipment, to provide the professional services and labor for installation of Lessee's equipment of an antenna and transmission line on Site Owner's Tower. This antenna is to be utilized by an amateur radio system and/or repeater system. The equipment, transmission line and equipment for this Amateur Radio system is not the financial responsibility of Lessee to provide and the labor only will be provided if the Equipment is present and available for installation at the time Lessee's equipment is installed. Lessee's only obligation is the placement of the antenna on the tower and the connection of the transmission line to the antenna with routing of the transmission line to the equipment shelter.

Tyler County Constable's

Six Month Summary

January - June 2012

Process Papers Served 264 \$21,120.00 to General Fund

Miles Patrolled 21,021

We have assisted the Tyler County Sheriff's Office as backup on Domestic Disturbances and other calls.

We have assisted DPS with wrecks and traffic stops.

We have conducted numerous building checks.

Deputy Constable and pct. 4 Constable worked as Bailiffs in County Court.

Deputy Constable mailed jury summons for District Court.

Deputy Constable mailed subpoenas for D.A.'s Office.

He also processed 2 seizures for the D.A.'s Office.

He also helped install and train on new metal detector for District Court.

He completed 24 hrs of training on Civil Process , Courtroom Security and Legislative update.

2nd qtr 2012

<u>Precinct#</u>			
1	2800	28	\$2,240.00
2	1374	16	\$1,280.00
3	1400	18	\$1,440.00
4	1850	17	\$1,360.00
Deputy	1650	52	\$4,160.00
Totals	9074	131	\$10,480.00

Gary Mattingly
Pct. 1 Constable

David Davis
Pct. 2 Constable

Jim Zachary
Pct. 4 Constable

Terry Riley
Deputy Constable

Wade Skinner
Pct. 3 Constable



GARRY MATTINGLY
CONSTABLE PCT 1

462 CR 4480

HOME PHONE: 409-547-3300

WARREN, TEXAS 77664

CELL PHONE: 409-429-4295

CONSTABLE'S REPORT

2nd quarter, 2012, papers served	28
Ending mileage	18,930
Beginning mileage	<u>16,330</u>
Total Mileage	2,800

Worked radar and patrolled Pct. 1, Tyler County and assisted when needed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Garry Mattingly".

Garry Mattingly

Constable, Pct.1



JIM ZACHARY

**CONSTABLE
TYLER COUNTY PCT #4**

P.O. Box 354
Spurger, TX. 77660

Office 409-429-3149
Cell 409-429-0509

2nd Qtr. Report 2012
Patrolled 1850 miles
Served 17 Civil Papers for \$1360 to General Fund.

Assisted other agencies including Sheriff's Office, DPS, Spurger VFD and other Constables on several calls.

Made numerous building checks.

Worked as Bailiff for County Court and Grand Jury Security.

Regards,

Jim Zachary
Tyler County Constable pct.4
tcc134@sbcglobal.net



TYLER COUNTY COMMISSIONERS COURT

County Courthouse, Room 101 / Woodville, Texas

Friday
July 13, 2012
8:30 AM

MARTIN NASH
Commissioner, Pct. 1

RUSTY HUGHES
Commissioner, Pct. 2

JACQUES L. BLANCHETTE
County Judge

MIKE MARSHALL
Commissioner, Pct. 3

JACK WALSTON
Commissioner, Pct. 4

NOTICE Is hereby given that a *Regular Meeting* of the Tyler County Commissioners Court will be held on the date stated above, at which time the following subjects will be discussed;

Agenda

"When you're more concerned about being politically correct, you compromise your responsibility to do the right thing."

➤ CALL TO ORDER

- Establish Quorum
- Acknowledge Guests
- Invocation *c/o M. Nash*
- Pledge to the Texas Flag: *c/o M. Nash*

"Honor the Texas Flag: I pledge allegiance to thee, Texas, one state under God, one and indivisible."

I. CONSIDER/APPROVE:

- TAB 1 Commissioners Court minutes** from previous meetings – *D. Gregory*
- Paying County bills** – *J. Skinner*
- TAB 2 Line item transfers / budget amendments** – *J. Skinner*
- One (1) year Airtime** for 12 Laptop Computers for Sheriff Department (ongoing yearly expense) – *J. Skinner*
- TAB 3** Joe Smith has reviewed. Contract is 59 pages long. Donece has a copy. **Contract Renewal** to the Attorney General of Texas Child Support Division FY 13/14 State Case Registry/Local Customer Service (SCR/LCS) Contract and pursuant to contract requirement {6.4.1.1} complete with Incident Response Plan – *Kim Nagypal, District Clerk*
- TAB 4 Resolution:** Grant 2590901 for "Software for Car Computers" Project to the Office of the Governor, Criminal Justice Division – *David Hennigan, Sheriff*
- Allowing installation of antennae** by Texas Forest Service on Tyler County's Doucette Tower – *Dale Freeman, Emergency Management*

H. TAB 5 Joe Smith has reviewed. **Communications Site Agreement** between Tyler County and Texas Forest Service – *D. Freeman*

I. Award Bids for the following equipment: 1997 GMC Dump Truck H1J5V00476; 1995 Chevrolet Cheyenne ½ ton pickup 1GCEC14HXSZ22885 – *M. Nash*

J. Award Bids for the following equipment: 1987 Ford Dump Truck 1FDXF82HXHVA65494; 1979 Oshkoch Army Truck 17298; 1999 Dodge Pickup 1B7HC16YXXS242273; 1997 Aerostar 7 Passenger Van 1FMCA11U2VZB15540; 25” Lowboy dual/tandem axle (weight empty 6880lbs.) NX04YS-2429 – *R. Hughes*

K. Appointment of Dr. Sandra Wright to represent Tyler County on the Regional Steering Committee - 1115 Medicaid Waiver / Region 2 – *J. Blanchette*

II. PRESENTATION

A. TAB 6 Report: Constable Quarterly Update – *Jim Zachary, Constable, Pct. 4*

B. Informational: Courthouse Security – *Terry Riley, Courthouse Security*

III. EXECUTIVE SESSION

Consult with District Attorney, Joe Smith, in executive session held in accordance with Texas Government Codes 555.071(1)(A), (2) regarding pending and/or contemplated litigation, and/or 551.074, regarding personnel matters, and/or property acquisition.

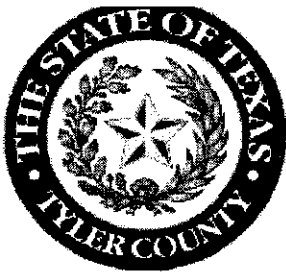
➤ ADJOURN

I do hereby certify that the above Notice of Meeting of the Tyler County Commissioners Court is a true and correct copy of said Notice and that I posted a true and correct copy of said Notice at the Tyler County Courthouse in a place readily accessible to the general public at all times and that said Notice remained so posted continuously for at least 72 hours preceding the scheduled time of said meeting, as is required by Section 551.002 & 551.041.

Executed on _____ 2012 Time _____

Donece Gregory, County Clerk/Ex Officio Member of Commissioners Court

By: _____ (Deputy)



TYLER COUNTY COMMISSIONERS COURT

County Courthouse, Room 101 / Woodville, Texas

Friday
July 13, 2012
8:30 AM

MARTIN NASH
Commissioner, Pct. 1

RUSTY HUGHES
Commissioner, Pct. 2

JACQUES L. BLANCHETTE
County Judge

MIKE MARSHALL
Commissioner, Pct. 3

JACK WALSTON
Commissioner, Pct. 4

NOTICE Is hereby given that a *Regular Meeting* of the Tyler County Commissioners Court will be held on the date stated above, at which time the following subjects will be discussed;

Agenda

"When you're more concerned about being politically correct, you compromise your responsibility to do the right thing."

➤ **CALL TO ORDER**

- Establish Quorum
- Acknowledge Guests
- Invocation *c/o M. Nash*
- Pledge to the Texas Flag: *c/o M. Nash*

"Honor the Texas Flag: I pledge allegiance to thee, Texas, one state under God, one and indivisible."

I. CONSIDER/APPROVE:

- A. **Commissioners Court minutes** from previous meetings – *D. Gregory*
- B. **Paying County bills** – *J. Skinner*
- C. **Line item transfers / budget amendments** – *J. Skinner*
- D. **One (1) year Airtime** for 12 Laptop Computers for Sheriff Department (ongoing yearly expense) – *J. Skinner*
- E. **Contract Renewal** to the Attorney General of Texas Child Support Division FY 13/14 State Case Registry/Local Customer Service (SCR/LCS) Contract and pursuant to contract requirement {6.4.1.1} complete with Incident Response Plan – *Kim Nagypal, District Clerk*
- F. **Resolution:** Grant 2590901 for "Software for Car Computers" Project to the Office of the Governor, Criminal Justice Division – *David Hennigan, Sheriff*
- G. **Allowing installation of antennae** by Texas Forest Service on Tyler County's Doucette Tower – *Dale Freeman, Emergency Management*
- H. **Communications Site Agreement** between Tyler County and Texas Forest Service – *D. Freeman*
- I. **Award Bids** for the following equipment: 1997 GMC Dump Truck HIJ5V00476; 1995 Chevrolet Cheyenne ½ ton pickup 1GCEC14HXSZ22885 – *M. Nash*
- J. **Award Bids** for the following equipment: 1987 Ford Dump Truck 1FDXF82HXHVA65494; 1979 Oshkoch Army Truck 17298; 1999 Dodge Pickup 1B7HC16YXXS242273; 1997 Aerostar 7 Passenger Van 1FMCA11U2VZB15540; 25" Lowboy dual/tandem axle (weight empty 6880lbs.) NX04YS-2429 – *R. Hughes*
- K. **Appointment** of Dr. Sandra Wright to represent Tyler County on the Regional Steering Committee - 1115 Medicaid Waiver / Region 2 – *J. Blanchette*

II. PRESENTATION

- A. **Report:** Constable Quarterly Update – *Jim Zachary, Constable, Pct. 4*
- B. **Informational:** Courthouse Security – *Terry Riley, Courthouse Security*

III. EXECUTIVE SESSION

Consult with District Attorney, Joe Smith, in executive session held in accordance with Texas Government Codes 555.071(1)(A), (2) regarding pending and/or contemplated litigation, and/or 551.074, regarding personnel matters, and/or property acquisition.

➤ **ADJOURN**

I do hereby certify that the above Notice of Meeting of the Tyler County Commissioners Court is a true and correct copy of said Notice and that I posted a true and correct copy of said Notice at the Tyler County Courthouse in a place readily accessible to the general public at all times and that said Notice remained so posted continuously for at least 72 hours preceding the scheduled time of said meeting, as is required by Section 551.002 & 551.041.

Executed on July 9th 2012 Time 3:05 pm
Donece Gregory, County Clerk/Ex Officio Member of Commissioners Court

By: [Signature] (Deputy)