State
Auditor's
Office

John Keel, CPA
State Auditor

An Audit Report on

Data Security Related to the Disposal of Surplus and Salvage State Data Processing Equipment at the Texas Department of Criminal Justice and Selected State Agencies

July 2011

Report No. 11-040

State Auditor's Office
John Keel, CPA
State Auditor

An Audit Report on

Data Security Related to the Disposal of Surplus and Salvage State Data Processing Equipment at the Texas Department of Criminal Justice and Selected State Agencies

SAO Report No. 11-040
July 2011

Overall Conclusion

There are risks associated with disposing of data processing equipment that state agencies and higher education institutions (state entities) should avoid by removing information prior to the equipment's disposal so that data recovery is not possible. State entities can choose to dispose of data processing equipment through the Texas Department of Criminal Justice's (TDCJ) Computer Recovery Program (Program) or on their own. In addition to releasing confidential information, state entities risk violating software licensing agreements and disclosing trade secrets, copyrights, and other intellectual property when disposing or transferring data processing equipment with storage devices to non-state entities.

Definitions

Data Processing - Information technology equipment and related services designed for the automated storage, manipulation, and retrieval of data by electronic or mechanical means.

Surplus Property - Personal property that exceeds a state entity's needs and is not required for the entity's foreseeable needs.

Salvage Property - Personal property that through use, time, or accident is so damaged, used, or consumed that it has no value for the purpose for which it was originally intended.

Sanitize - A process to remove information from media so that data recovery is not possible.

Confidential Information - Information that must be protected from unauthorized disclosure or public release based on state or federal law.

The TDCJ Program properly sanitized and substantially destroyed computer hard drives it received from state entities, school districts, and other political subdivisions. Sanitizing is the removal of data from media such as hard drives or other storage devices using methods to ensure that data recovery is not possible (see text box for definitions of related terms). However, TDCJ does not have procedures in place to identify all types of data processing equipment that contain storage devices—such as printers, copiers, or scanners—so that they can be sanitized. In addition, TDCJ should improve its processes to (1) verify that it receives all data processing equipment intended for the Program and (2) safeguard the physical security of the data processing equipment it receives.

The Program did not recover TDCJ's costs as required by Texas Government Code, Section 497.012 (related to the repair and resale of surplus data processing equipment), during fiscal years 2008 through 2010. The Program provides at no cost disposal services to state entities and refurbished data processing equipment

This audit was conducted in accordance with Texas Government Code, Section 321.0132.

For more information regarding this report, please contact Sandra Vice, Assistant State Auditor, or John Keel, State Auditor, at (512) 936-9500.

to school districts and other political subdivisions. During fiscal years 2008 through fiscal year 2010:

- State entities relied on the TDCJ Program to dispose of 128,111 (66.8 percent) of the 191,814 items of data processing equipment they disposed, according to data from the State Property Accounting system.

- The Program provided 16,144 computers, printers, and scanners to 94 school districts and other political subdivisions in Texas.

- The Program recovered 23.3 percent of its costs; the program cost $3,338,690 to operate and generated $779,459 in revenue from scrap material sales.

Auditors also reviewed the disposal processes at two agencies and identified weaknesses that should be addressed to ensure that confidential data is protected. Specifically:

- The Texas Commission on Environmental Quality (TCEQ) did not properly sanitize its data processing equipment in compliance with state laws and rules. Of the 30 hard drives that auditors tested at TCEQ, 29 (96.7 percent) contained recoverable data, and some of those hard drives contained confidential data. TCEQ has taken steps to address this deficiency and management asserted that those 29 hard drives were subsequently sanitized before being transferred to non-state entities. In addition, TCEQ did not have procedures to identify and sanitize all equipment with storage devices.

- The Texas Parks and Wildlife Department (TPWD) properly sanitized computer hard drives prior to transferring the equipment to state and non-state entities; however, it could improve its processes to ensure that all hard drives go through the sanitization process. In addition, TPWD did not have procedures to identify and sanitize all equipment with storage devices.

Texas Government Code, Section 2054.130, requires state entities to permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment outside of state property. State entities can find a link to a list of free software tools to sanitize data in the Department of Information Resources' *Sale or Transfer of Computers and Software Guidelines*.

Senate Bill 1 (82nd Legislature, 1st Called Session) would amend Texas Government Code, Chapter 2175, and make the Texas Facilities Commission responsible for the disposal of surplus and salvage property in Texas. The process outlined in this report may change as a result of the passage of Senate Bill 1. As of the release of this audit report, Senate Bill 1 was awaiting action by the Governor.

Summary of Management's Response

Management at the three agencies audited agreed with the findings and recommendations in this report. The agencies' detailed management responses are presented immediately following each set of recommendations in the Detailed Results section of this report.

Summary of Objective, Scope, and Methodology

The objective of this audit was to determine whether the Program and selected state entities remove or destroy data from electronic storage devices prior to the devices' sale, transfer, or destruction in accordance with state law, administrative rules, and state entity policies and procedures.

The scope of this audit included the inventory of data processing equipment at the Program at the times auditors were on site, as well as the inventory of data processing equipment at TCEQ and TPWD that was available for transfer to other state entities or was available for sale to the public during fieldwork. The audit covered financial information provided by TDCJ for the Program for fiscal years 2008 through 2010.

The audit methodology included reviewing applicable laws, regulations, and guidelines; reviewing internal policies and procedures; interviewing key program personnel; testing hard drives from data processing equipment; and reviewing selected documentation.

Auditors determined that TDCJ's financial information related to the Program for fiscal year 2010 was sufficiently reliable for the purposes of this report. Auditors interviewed personnel knowledgeable about the systems. In addition, auditors tested key access and application controls over the systems.

Auditors also relied on prior audit work the State Auditor's Office conducted to assess the reliability of the State Property Accounting system (SPA). Auditors determined that SPA data was sufficiently reliable for the purposes of this audit.

Auditors also communicated less significant issues to TDCJ, TCEQ, and TPWD separately in writing.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

TDCJ's Computer Recovery Program Properly Sanitized and Substantially Destroyed Computer Hard Drives; However, It Should Verify That It Receives All Equipment and Destroys or Sanitizes Storage Devices in Other Data Processing Equipment

Computer Recovery Program

TDCJ's Computer Recovery Program (Program) was established in 1999 and allows state entities, school districts, and other political subdivisions to send surplus or salvage data processing equipment to TDCJ, which refurbishes or recycles the equipment. TDCJ offers refurbished equipment at no cost to state entities, school districts, and other political subdivisions.

Program facilities are located at the Price Daniel Unit in Snyder and at the John M. Wynne Unit in Huntsville.

The Program also sells scrap data processing material to defray the costs of operating the program.

Source: Texas Correctional Industries Web site.

The Texas Department of Criminal Justice's (TDCJ) Computer Recovery Program (Program):

- Properly sanitized computer hard drives it received from state agencies and higher education institutions (state entities), school districts, and other political subdivisions prior to transferring refurbished data processing equipment to state entities, school districts, and other political subdivisions.
- Destroyed hard drives completely at the John M. Wynne Unit in Huntsville (Wynne Unit), but it should improve its destruction process at the Price Daniel Unit in Snyder (Daniel Unit).
- Did not adequately verify that it received all data processing equipment sent from state entities, school districts, and other political subdivisions.
- Did not have procedures in place to identify all data processing equipment with a storage device, such as printers, copiers, scanners, fax machines, and personal digital assistants.
- Did not track inventory tags given to Freight Transportation department personnel, and Freight Transportation department personnel did not record the inventory tag numbers used during deliveries.
- Did not earn enough from the sale of scrap data processing material to defray the costs of operating the Program. According to TDCJ, the Program provided 16,144 computers, printers, and scanners to 94 school districts and other political subdivisions from fiscal year 2008 through fiscal year 2010.

TDCJ receives data processing equipment from state entities, school districts, and political subdivisions (see text box). TDCJ personnel remove computer hard drives from computers, sanitize those hard drives intended for use in refurbished computers, and destroy those hard drives designated as salvage. Table 1 on the next page lists the total number of data processing equipment TDCJ received from state entities in fiscal years 2008 through 2010. State entities disposed of 128,111 items of data processing equipment through the Program from fiscal year 2008 through fiscal year 2010, according to data from the State Property Accounting system. During that same time period, state entities disposed of a total of 191,814 items of data processing equipment; the state entities used the Program to dispose of 66.8 percent of those items (see Appendix 2 for more information about the amount of data processing equipment disposed).

Table 1

Equipment That TDCJ Received from State Entities Through Its Computer Recovery Program [a]
Fiscal Year 2008 through Fiscal Year 2010

Type of Equipment	Fiscal Year in Which Equipment Was Disposed			Total
	2008	2009	2010	
Desktop Computer	35,577	32,471	28,974	97,022
Laptop Computer	3,876	6,134	4,621	14,631
Printer, Copier, Scanner, Fax Machine, or Personal Digital Assistant	5,066	4,709	4,218	13,993
Server	700	924	841	2,465
Totals	**45,219**	**44,238**	**38,654**	**128,111**

[a] The Office of the Comptroller of Public Accounts' (Comptroller) State Property Accounting system does not track transfers of equipment from school districts or political subdivisions.

Source: Comptroller's State Property Accounting system.

Chapter 1-A

TDCJ Properly Sanitized Hard Drives Received from State Entities, School Districts, and Other Political Subdivisions

The settings on the hardware devices that TDCJ uses to sanitize hard drives received from state entities, school districts, and other political subdivisions comply with state laws and rules and the *National Industrial Security Program Operating Manual* (DoD 5220.22-M), which provides guidelines on clearing and sanitizing data processing equipment.

Auditors tested 30 hard drives that had been marked as sanitized at the Wynne Unit and 30 hard drives at the Daniel Unit. TDCJ properly sanitized all 60 hard drives tested and auditors were not able to retrieve data from any hard drive tested.

TDCJ installs an operating system on each refurbished computer to verify that the computer is working properly. Afterward, TDCJ sanitizes each hard drive a second time to ensure that school districts and other political subdivisions receive a computer containing no retrievable data. Auditors determined that

TDCJ properly documented that each hard drive was sanitized a second time prior to a hard drive's transfer to state entities, school districts, and other political subdivisions.

Chapter 1-B

TDCJ Should Improve Its Procedures to Verify That It Receives All Data Processing Equipment Intended for the Program

TDCJ should improve its procedures to verify that it receives all data processing equipment intended for the Program. Currently, state entities, school districts, and other political subdivisions must complete and submit to the Program a data processing equipment transfer information form and a bill of lading form prior to TDCJ picking up the surplus and salvage computer equipment. When the data processing equipment reaches the Program, TDCJ employees verify they have received the same number of pallets as listed on the forms. However, TDCJ employees do not verify that the pallets contain the same number of data processing equipment items as the number reported shipped.

While the entities transferring data processing equipment completed the required forms, they were inconsistent about what information they included on the forms. The bill of lading form includes columns for serial numbers and property tag numbers, but the instructions state that entities are not required to submit that information. Without that information, TDCJ employees cannot verify that the Program received all data processing equipment intended for the Program.

In addition, 32 (80.0 percent) of 40 data processing items disposed by the Wynne Unit were not recorded as disposed through the Program by state entities in the Comptroller's State Property Accounting system. Specifically:

- Twenty-six items had no disposal code in the State Property Accounting system; as a result, the items were not recorded as disposed by the state entity.

- Six items were incorrectly recorded as salvage or dismantled for parts by the state entity.

Five (16.7 percent) of 30 data processing items disposed by the Daniel Unit were either not recorded as disposed through the Program by state entities or auditors could not identify the items in the State Property Accounting system. Specifically:

- One item was incorrectly recorded as salvage or dismantled for parts by the state entity.

- Auditors could not determine whether four items were properly recorded as disposed through the Program because the identifying numbers recorded in the bill of lading were not state property tag numbers. TDCJ does not require property tag numbers to be recorded in the bill of lading.

TDCJ could help ensure that the disposition of data processing equipment is properly recorded in the Comptroller's State Property Accounting system by requiring an entity to provide documentation that it has recorded the data processing equipment as disposed through the Program in the State Property Accounting system.

Chapter 1-C

TDCJ Does Not Have Processes in Place to Identify All Data Processing Equipment with a Storage Device, Such as Printers, Copiers, Scanners, Fax Machines, and Personal Digital Assistants

In addition to desktop and laptop computers, TDCJ refurbishes and donates printers, copiers, scanners, fax machines, and personal digital assistants, some of which may contain a storage device. TDCJ transfers those types of equipment to school districts and other political subdivisions. Auditors conducted an Internet search on unique (different make and model) surplused printers, copiers, scanners, and fax machines available for transfer at TDCJ at the time auditors were on site to determine whether the equipment may contain a storage device (there were no personal digital assistants available during testing).

Internet sources indicated that 10 (33.3 percent) of 30 unique printers, copiers, scanners, and fax machines at the Wynne Unit and 10 (50.0 percent) of 20 unique printers, copiers, and scanners at the Daniel Unit may contain a storage device. Auditors tested four printers to determine whether they contained a storage device (two printers at the Wynne Unit and two printers at the Daniel Unit), and none contained a storage device. TDCJ management stated that Program employees conduct random searches for storage devices in printers, copiers, scanners, fax machines, and personal digital assistants. However, TDCJ does not have policies and procedures in place to ensure that employees inspect all printers, copiers, scanners, fax machines, and personal digital assistants for storage devices, which increases the risk that employees will not inspect those types of equipment in a consistent manner.

Texas Government Code, Section 2054.130, and Title 1, Texas Administrative Code, Section 202.28, together require state agencies to permanently remove restricted personal information, confidential information, mission-critical information, intellectual property, and licensed software from all data storage devices or destroy the devices before an agency disposes of the equipment or transfers it to a person who is not representing a state agency or other agent of the State. If TDCJ does not ensure that printers, copiers, scanners, fax machines, and personal digital assistants are consistently inspected and that storage devices are removed and sanitized or destroyed, there is an increased risk that the equipment transferred to school districts and other political subdivisions may contain retrievable confidential and/or sensitive data.

Chapter 1-D

TDCJ's Wynne Unit Properly Destroyed All Salvage Hard Drives, But TDCJ Should Improve Its Processes at the Daniel Unit

The Wynne Unit properly destroyed all 30 hard drives tested that were ready to be sold as salvage equipment. However, the Daniel Unit should improve its processes for destroying salvage equipment. According to policies and procedures at the Daniel Unit, all hard drives that will not boot, fail during testing, or do not meet the minimum requirements must be designated as salvage and destroyed using a hammer. The Daniel Unit properly destroyed 29 (96.7 percent) of 30 hard drives ready to be sold as salvage equipment that auditors reviewed. One hard drive did not show any physical evidence that it had been struck with a hammer. Although auditors reviewed the contents of the hard drive and were not able to recover data from it, the risk exists that salvage equipment that is not properly destroyed could contain recoverable data; TDCJ does not conduct reviews of salvage hard drives to verify that they were properly destroyed prior to sale.

The Program at the Daniel Unit does not have the same equipment to destroy hard drives as the Program at the Wynne Unit. Specifically:

- At the Wynne Unit, a hard drive is placed in a vise-like device that holds it so that half of the hard drive is exposed, and the hard drive is struck with a hammer, breaking the platters that store data within it. This process provides visible evidence that a hard drive has been properly destroyed.

- At the Daniel Unit, a hard drive is placed on a table or the floor and struck with a hammer. This method does not provide as much visible evidence that the platters within the hard drive were destroyed.

Confidential information could be released from salvage hard drives if those hard drives are not properly destroyed. Auditors tested a sample of 30 hard drives donated from a public school district and determined that all 30 hard drives contained retrievable data upon arrival at the Daniel Unit. It is critical that TDCJ ensures that the Program properly destroys or sanitizes all hard drives to prevent confidential information and other data from being compromised.

Chapter 1-E

TDCJ Does Not Track or Reconcile Inventory Tags Placed on Delivery Truck Doors to Deter and Detect Tampering

The TDCJ Freight Transportation department picks up computer devices from donating entities and transports the equipment to one of the Program's two units in Huntsville and Snyder. Inventory tags are placed on the delivery truck doors during any unscheduled stops while en route to a unit. Freight Transportation department personnel may remove an inventory tag to inspect the trailer. If a tag is broken or otherwise altered by anyone other than Freight Transportation department personnel, this indicates that someone tampered with the trailer while en route to the Program. However, TDCJ's procedures are not sufficient to consistently track inventory tags. Specifically, TDCJ does not track inventory tag numbers given to Freight Transportation department personnel, and Freight Transportation department personnel do not record the inventory tag numbers used during deliveries.

At the Wynne Unit, the Freight Transportation department delivers the equipment directly to the Program. However, if the delivery truck arrives after the Program's work hours, the Freight Transportation department leaves the trailer outside the prison walls. At the Daniel Unit, all deliveries are received by the TDCJ Snyder Distribution Center. If only a few pallets are designated for the Program, those pallets are unloaded into the warehouse. But if the entire shipment is designated for the Program, the trailer will remain parked in the distribution center's parking lot overnight.

TDCJ's procedures for the inspection and verification of inventory tag numbers are inconsistent. Specifically:

- At the Wynne Unit, Freight Transportation department personnel document the inventory tag number, which they list in a data processing equipment shipping information form, only if they have to leave the trailer outside the prison walls. Wynne Unit prison guards then verify that the inventory tag matches the number documented in the data processing equipment shipping information form prior to allowing the truck to deliver its equipment to the Program.

- The Daniel Unit does not document the inventory tag number at any point from pick-up to delivery.

The Comptroller's *State Property Accounting Process User's Guide* states that "each agency is responsible for ensuring that property is tracked and secured in a manner that is most likely to prevent theft, loss, damage, or misuse. The agency must take all necessary precautions to ensure that property is secured." If TDCJ does not track and verify the inventory tag numbers on data processing equipment being transported to the Program, there is an increased risk of theft or misconduct related to those shipments to the Program.

Chapter 1-F

The Sales Price of the Components and Equipment Does Not Defray the Program's Full Repairing, Refurbishing, or Disassembling Costs

TDCJ receives revenue from the Program's sale of scrap data processing material; however, the revenue was not sufficient to cover the expenditures incurred by the Program in fiscal years 2008 through 2010. During this same time period, the Program recovered 23.3 percent ($779,459 out of $3,338,690) of the Program costs. Table 2 lists the Program's revenues from the sale of scrap data processing material and total expenditures for fiscal years 2008 through 2010.

Table 2

Program Revenue from Sale of Scrap Material and Expenditures
Fiscal Years 2008 through 2010

Fiscal Year	Revenue	Expenditures	Difference
2008	$ 328,310	$ 1,095,481	($767,171)
2009	175,725	1,139,657	(963,932)
2010	275,424	1,103,552	(828,128)
Totals	**$779,459**	**$3,338,690**	**($2,559,231)**

Source: TDCJ.

Of the Program's $3,338,690 in total expenditures for fiscal years 2008 through 2010:

- Payroll accounted for 68.6 percent (or $2,290,635). TDCJ has seven employees at the Wynne Unit and eight employees at the Daniel Unit. Texas Government Code, Section 497.012, states that TDCJ employees shall remove and sanitize storage devices from surplus or salvage data processing equipment before offenders can access the equipment. TDCJ employees are responsible for removing and sanitizing the hard drives from donated computers; offenders are responsible for repairing, refurbishing, and testing the equipment to verify that it is working properly.

- Transportation accounted for 13.3 percent (or $444,375). TDCJ's Freight Transportation department is responsible for picking up donated equipment and shipping refurbished equipment. The Freight Transportation department charges the Program based on the number of miles assigned to the order. According to TDCJ, the Program was charged for 197,366 miles from fiscal years 2008 through 2010.

- Depreciation accounted for 9.7 percent (or $323,606). The Program depreciated a building, a chilled water machine, two shrink-wrap machines, a forklift, a pickup truck, and two hard drive sanitization machines from fiscal years 2008 through 2010.

- Parts and maintenance, consumables, utilities, and other costs accounted for the remaining 8.4 percent (or $280,074).

Texas Government Code, Section 497.012, which is the enabling legislation for the Program, states:

> "[TDCJ] shall sell the repaired or refurbished data processing equipment to a school district, a state agency, or a political subdivision ... The sales price of the components or the repaired or refurbished data processing equipment must be sufficient to defray the cost of repairing, refurbishing, or disassembling the data processing equipment."

TDCJ does not collect any revenue for refurbished data processing equipment donated to school districts and other political subdivisions. According to TDCJ, the Program provided 16,144 computers, printers, and scanners to 94 school districts and other political subdivisions from fiscal year 2008 through fiscal year 2010 (see Table 3).

Table 3

Refurbished Computers, Printers, and Scanners That TDCJ's Computer Recovery Program Donated to School Districts and Political Subdivisions
Fiscal Years 2008 through 2010

Entity That Received Refurbished Equipment	Equipment Sent		Total Equipment Donated	Total Number of Recipients
	Wynne Unit	Daniel Unit		
School Districts	8,528	7,469	15,997	80
Political Subdivisions	18	129	147	14
Totals	**8,546**	**7,598**	**16,144**	**94**

Source: Wynne Unit and Daniel Unit databases for outgoing shipments from the Program.

Recommendations

TDCJ should:

- Require entities transferring data processing equipment to list, at a minimum, in the bill of lading form the type and quantity of computer equipment being sent to the Program.

- Verify that it received all data processing equipment for randomly selected pallets.

- Require state entities transferring data processing equipment to provide verification that the equipment is properly recorded as disposed through the Program in the State Property Accounting system.

- Develop and implement policies and procedures related to identifying storage devices from non-computer devices, such as printers, copiers, scanners, fax machines, and personal digital assistants.

- Obtain and use a hard drive vise for destroying salvage hard drives at the Daniel Unit.

- Visually inspect salvage hard drives to verify that they have been destroyed prior to sale.

- Develop and implement policies and procedures that establish when inventory tags should be used, and require Freight Transportation department employees to record the inventory tag number every time a tag is placed on a trailer. The policies and procedures also should require program personnel to compare the inventory tag numbers on delivery trucks to the numbers recorded by the Freight Transportation department.

- Make changes to its Program to decrease its expenditures and increase its revenue sources with the goal of recovering the Program's operating costs, as required by statute. Changes may include:

  - Reducing expenditures by operating the Program more efficiently.

  - Increasing revenue by charging a fee—to be determined by TDCJ—to state entities, school districts, or other political subdivisions for sanitization and disposal services.

  - Either requiring entities receiving donated data processing equipment from the Program to pick up the equipment or charging them a delivery fee.

Management's Response

- *TDCJ should require entities transferring data processing equipment to list, at a minimum, in the bill of lading form the type and quantity of computer equipment being sent to the Program.*

  Response: Agree.

  The TDCJ will require the Manufacturing and Logistics (M&L)-114 form (Bill of Lading) be fully completed. The facility will assess an entity's M&L-114 form for completeness upon receipt. If any information is lacking or needs to be revised, the donating entity will be notified to *correct the information on the form prior to the data processing equipment being picked up by the TDCJ. A Standard Operating Procedure (SOP) will be written to implement this requirement. Each facility manager will be responsible for implementing the SOP. This will be completed by September 1, 2011.*

- *Verify that it received all data processing equipment for randomly selected pallets.*

  Response: Agree.

  Random pallet inventories will be performed after the pallet count from the truck has been verified and the pallet has been searched for contraband. The M&L-114 forms will be reviewed and cross checked against the pallet contents. Any discrepancies will be noted on the M&L-114 forms and the donating entity will be notified of the discrepancy. An SOP will be written to implement this requirement. Each facility manager will be responsible for implementing the SOP. This will be completed by September 1, 2011.

- *Require state entities transferring data processing equipment to provide verification that the equipment is properly recorded as disposed through the Program in the State Property Accounting system.*

  Response: Agree.

  An additional requirement will be added to the M&L-114 form which requires the donating entity to indicate that the data processing equipment has been properly recorded as disposed of in the State Property Accounting (SPA) system. Any discrepancies will be noted on the M&L-114 forms and the donating entity will be notified of the discrepancy. The Manager for Offender Work and Training Programs will be responsible for this and it will be completed by September 1, 2011.

- *Develop and implement policies and procedures related to identifying storage devices from non-computer devices, such as printers, copiers, scanners, fax machines and personal digital assistants.*

  Response: Agree.

  An SOP will be written to establish procedures to assess all incoming data processing equipment for possible data storage devices. A list will be generated and updated at both facilities that identify current manufacturers and models that contain internal storage devices. M&L Information Technology department may be contacted by either facility to assist in determining if equipment has a data storage device. Each facility *manager will be responsible for implementing the SOP. This will be completed by September 1, 2011.*

- *Obtain and use a hard drive vise for destroying salvage hard drives at the Daniel Unit.*

  Response: Agree.

  Daniel Computer Recovery now has a device to properly destroy hard drives. An SOP has been written and implemented to ensure all scrap hard drives have been properly destroyed. This was completed on June 24, 2011.

- *Visually inspect salvage hard drives to verify that they have been destroyed prior to sale.*

  Response: Agree.

  An SOP was implemented on June 24, 2011 that requires visual inspection to ensure destruction.

- *Develop and implement policies and procedures that establish when inventory tags should be used and require freight transportation department employees to record the inventory tag number every time a tag is placed on a trailer. The policies and procedures also should require program personnel to compare the inventory tag numbers on delivery trucks to the numbers recorded by the freight transportation department.*

  Response: Agree.

  The security seals are referenced in Post Order-07.054 (back gate officer) for trucks leaving the unit. The TDCJ will develop and implement policies and procedures to clarify all instances when a security seal on a trailer with salvage computer equipment is to be used and how verification of the seal is to occur. We will also establish a process to track the seals to ensure they can be properly reconciled. This will be completed by September 1, 2011 by the Assistant Director for Transportation and Supply.

- *Make changes to its Program to decrease its expenditures and increase its revenue sources with the goal of recovering the Program's operating costs, as required by statute. Changes may include:*

  - *Reducing expenditures by operating the program more efficiently.*

  - *Increasing revenue by charging a fee--to be determined by the TDCJ--to state entities, school districts, or other political subdivisions for sanitization and disposal services.*

- *<u>Either requiring entities receiving donated data processing equipment from the Program to pick up the equipment or charging them a delivery fee.</u>*

Response: Agree.

- *The TDCJ will continue to review the Program to ensure operational efficiency and will reduce costs whenever possible.*
- *The TDCJ will consult with the legislature regarding implementation of a fee for sanitization and disposal services that would be assessed per computer system to help defray operating expenses.*
- *The TDCJ will consult with the legislature regarding implementation of a fee for delivery of the refurbished computer equipment or requiring that the receiving entity pick up the equipment from the facility.*

Chapter 2

TCEQ Did Not Properly Sanitize Its Data Processing Equipment in Compliance with State Laws and Rules

Surplus Data Processing Equipment

The TCEQ posts surplus data processing equipment on the Comptroller's Web site for 10 business days. If interested in a piece of equipment, a state entity, political subdivision, or assistance organization may coordinate with TCEQ for a transfer of the equipment. A transfer to a state agency has priority over any other transfers during the 10-day period that the equipment is listed on the Comptroller's Web site.

After 10 business days have passed, TCEQ may transfer the equipment to a school district or open-enrollment charter school, an assistance organization, or TDCJ.

Sources: Texas Government Code, Sections 2175.128 and 2175.184; *TCEQ Guide for Administrative Procedures Manual*.

The Texas Commission on Environmental Quality (TCEQ) did not meet the standards established by state laws and rules and U.S. Department of Defense guidelines when it sanitized computer hard drives in surplus equipment. TCEQ has taken steps to address this deficiency. In addition, TCEQ did not have specific processes in place to identify and either destroy or sanitize all data processing equipment that may contain a storage device, such as printers, scanners, servers, and personal digital assistants. TCEQ recorded the correct disposition code for disposed equipment in the Comptroller's State Property Accounting system. TCEQ could improve how it documents the process and sanitization tools it used to remove data from or to destroy storage devices.

TCEQ may transfer its surplus equipment to state entities, political subdivisions, or assistance organizations (see text box). Table 4 lists the types and totals of TCEQ's disposed data processing equipment for fiscal years 2008 through 2010.

Table 4

TCEQ's Disposed Data Processing Equipment
Fiscal Years 2008 through 2010

Type of Equipment	Fiscal Year in Which Equipment Was Disposed			Total
	2008	2009	2010	
Desktop Computer	496	592	664	1,752
Laptop Computer	136	92	79	307
Printer, Scanner, or Personal Digital Assistant	64	231	298	593
Server	30	41	23	94
Totals	**726**	**956**	**1,064**	**2,746**

Source: Comptroller's State Property Accounting system.

Chapter 2-A

The Process That TCEQ Used to Sanitize Hard Drives Did Not Meet the Standards for Disposal of Potentially Confidential Data

TCEQ did not comply with the standards established in state laws and rules and the *National Industrial Security Program Operating Manual* (DoD

5220.22-M)[1] when it sanitized the hard drives in surplus data processing equipment prior to transferring the equipment to state entities, political subdivisions, or assistance organizations. Of the 30 hard drives prepared for transfer that auditors tested, 29 (96.7 percent) contained recoverable data, and some of those hard drives contained confidential data. TCEQ has taken steps to address this deficiency and management asserted that those 29 hard drives were subsequently sanitized before being transferred to non-state entities.

Texas Government Code, Section 2054.130, and Title 1, Texas Administrative Code, Section 202.28, together require state agencies to permanently remove restricted personal information, confidential information, mission-critical information, intellectual property, and licensed software from all data storage devices or destroy the devices before an agency disposes of the equipment or transfers it to a person who is not representing a state agency or other agent of the State. If TCEQ does not ensure that all hard drives are properly sanitized, there is an increased risk that equipment transferred to political subdivisions or assistance organizations may contain retrievable confidential and/or sensitive data.

Since the conclusion of auditors' testing, TCEQ has taken steps to address the deficiencies discussed above. TCEQ has drafted new policies and procedures for the sanitization of hard drives and acquired software specifically designed to sanitize hard drives.

Chapter 2-B

TCEQ Did Not Have Specific Processes to Identify and Sanitize All Data Processing Equipment with a Storage Device, Including Printers, Scanners, Servers, and Personal Digital Assistants

In addition to desktop and laptop computers, TCEQ surpluses printers, scanners, servers, and personal digital assistants, some of which may contain storage devices. TCEQ transfers these types of equipment to political subdivisions or assistance organizations. Auditors conducted an Internet search on the surplused printers, servers, and personal digital assistants available during audit fieldwork at the TCEQ warehouse to determine whether the equipment may contain a storage device (there were no scanners available during testing).

Internet sources indicated that 3 (37.5 percent) of 8 printers designated as surplus that auditors reviewed may contain a hard drive. Auditors also identified two servers containing hard drives and one personal digital assistant model that contained a storage device. Auditors did not test the three printers, two servers, or personal digital assistant to determine whether they actually

[1] The *National Industrial Security Program Operating Manual* (DoD 5220.22-M) provides guidelines on clearing and sanitizing data processing equipment that may contain sensitive or confidential information.

contained storage devices. However, TCEQ does not have policies and procedures that specifically address the identification, destruction, and sanitization of storage devices that may be contained within printers, scanners, servers, and personal digital assistants.

If TCEQ does not inspect, remove, and sanitize storage devices in printers, scanners, servers, and personal digital assistants, there is an increased risk that equipment transferred to non-state entities may contain retrievable confidential and/or sensitive data.

Chapter 2-C

TCEQ Recorded Disposed Equipment Correctly in the Statewide System, But It Could Improve How It Documents Required Information for Salvage or Surplus State Data Processing Equipment

TCEQ correctly recorded in the Comptroller's State Property Accounting system whether equipment was acquired by non-state entities for all 30 disposal forms tested.

In addition, the form that TCEQ used to document the disposal of data processing equipment includes many but not all of the required elements in Title 1, Texas Administrative Code, Section 202.28. Specifically, TCEQ documents:

- Include the date of disposal, description of salvage or surplus items, serial numbers, inventory numbers, and names and addresses of the organizations to which the equipment was transferred (if applicable).
- Do not include the process and sanitization tools used to remove the data or method of destruction. TCEQ could not provide auditors documentation showing the sanitization tools or the destruction methods used because that information is not being collected.

Recommendations

TCEQ should:

- Obtain and use readily available software or hardware for sanitizing hard drives in compliance with the standards set by the *National Industrial Security Program Operating Manual* (DoD 5220.22-M).
- Develop and implement policies and procedures that comply with Title 1, Texas Administrative Code, Section 202.28, which requires that agencies properly sanitize hard drives contained within data processing equipment prior to the equipment's transfer or disposal.

- Develop and implement policies and procedures to inspect all data processing equipment, including printers, scanners, servers, and personal digital assistants to identify, remove, and sanitize all internal hard drives prior to the equipment being surplused.
- Document the process and sanitization tools it used to remove data from salvage or surplus data processing equipment or the methods used to destroy the equipment.

Management's Response

- *TCEQ should obtain and use readily available software or hardware for sanitizing hard drives in compliance with the standards set by the National Industrial Security Program Operating Manual (DoD 5220.22-M).*

  TCEQ concurs with this recommendation and acquired software, DBAN, recommended by the Texas Department of Information resources in April 2011 to comply with the standards set by the National Industrial Security Program Operating Manual (DoD 5220.22-M). TCEQ staff routinely test to ensure that no data is recoverable after sanitizing with this product. Responsible party: Customer Support Center Section Manager.

- *Develop and implement policies and procedures that comply with Title 1, Texas Administrative Code, Section 202.28, which requires that agencies properly sanitize hard drives contained within data processing equipment prior to the equipment's transfer or disposal.*

  TCEQ concurs with this recommendation and developed policies and procedures that were put in place in May 2011 that outline the agency's compliance with Title 1, Texas Administrative Code, Section 202.28. Additionally, the agency's Guide to Administrative Procedures manual section pertaining to the surplus of electronic storage devices will be updated by July 31, 2011. Responsible party: Customer Support Center Section Manager.

- *Develop and implement policies and procedures to inspect all data processing equipment, including printers, scanners, servers, and personal digital assistants to identify, remove, and sanitize all internal hard drives prior to the equipment being surplused.*

  TCEQ concurs with this recommendation and believes that the policies and procedures developed for the recommendation above will address the electronic storage devices used in printers and servers. TCEQ does not own any scanners with electronic storage devices. TCEQ will develop a policy and procedure for the sanitization or destruction of personal digital *assistants by August 31, 2011. Responsible party: Customer Support Center Section Manager.*

- *Document the process and sanitization tools it used to remove data from salvage or surplus data processing equipment or the methods used to destroy the equipment.*

  TCEQ concurs with this recommendation and documented the process and sanitization tools in a Standard Operating Procedure in the Customer Service Section of the Information Resources Division in May 2011. Responsible party: Customer Support Center Section Manager.

Chapter 3

TPWD Properly Sanitized Computer Hard Drives Prior to Transfer; However, It Should Improve Its Processes to Identify All Equipment with Storage Devices

The Texas Parks and Wildlife Department (TPWD) uses a hardware device to sanitize surplus computer hard drives that complies with state laws and rules, as well as with U.S. Department of Defense guidelines. TPWD could improve its processes by verifying that all hard drives go through the sanitization process and destroying or sanitizing the storage device on all data processing equipment, such as printers, copiers, servers, and fax machines. TPWD recorded the correct disposition code for disposed equipment in the State Property Accounting system. TPWD could improve how it documents the process and sanitization tools it used to remove data from or to destroy storage devices.

Surplus Data Processing Equipment

The TPWD posts surplus data processing equipment on the Comptroller's Web site for 10 business days. If interested in a piece of equipment, a state entity, political subdivision, or assistance organization may coordinate with TPWD for a transfer of the equipment. A transfer to a state agency has priority over any other transfers during the 10-day period that the equipment is listed on the Comptroller's Web site.

After 10 business days have passed, TPWD may transfer the equipment to a school district or open-enrollment charter school, an assistance organization, or TDCJ.

Sources: Texas Government Code, Sections 2175.128 and 2175.184.

TPWD may transfer its surplus equipment to state entities, political subdivisions, or assistance organizations (see text box). In addition, TPWD transfers printers, copiers, servers, and fax machines to the Texas Facilities Commission's State Surplus storefront, where they are available for sale to the public. Table 5 lists the types and totals of TPWD's disposed data processing equipment for fiscal years 2008 through 2010.

Table 5

TPWD's Disposed Data Processing Equipment
Fiscal Years 2008 through 2010

	Fiscal Year in Which Equipment Was Disposed			
Type of Equipment	2008	2009	2010	Total
Desktop Computer	451	412	768	1,631
Laptop Computer	226	53	161	440
Printer, Copier, or Fax Machine	96	26	119	241
Server	42	4	9	55
Totals	**815**	**495**	**1,057**	**2,367**

Source: Comptroller's State Property Accounting system.

Chapter 3-A

TPWD Has a Process to Properly Sanitize Hard Drives; However, It Should Verify That All Hard Drives Complete the Process

The hardware device that TPWD uses to sanitize surplus hard drives and its settings comply with state laws and rules and the *National Industrial Security Program Operating Manual* (DoD 5220.22-M), which provides guidelines on clearing and sanitizing data processing equipment.

Of the 30 hard drives that had been marked as sanitized that auditors tested, TPWD properly sanitized 29 (96.7 percent). One hard drive had been marked as sanitized even though it had not gone through the sanitizing process. Auditors were able to retrieve data from the hard drive but did not identify any confidential information in the retrieved data**.** TPWD employees do not conduct periodic reviews of sanitized hard drives to verify that the equipment is being properly sanitized.

Texas Government Code, Section 2054.130, and Title 1, Texas Administrative Code, Section 202.28, together require state agencies to permanently remove restricted personal information, confidential information, mission-critical information, intellectual property, and licensed software from all data storage devices or destroy the devices before an agency disposes of the equipment or transfers it to a person who is not representing a state agency or other agent of the State. If TPWD does not ensure that all hard drives are properly sanitized, there is an increased risk that equipment transferred to assistance organizations may contain retrievable confidential and/or sensitive data.

Chapter 3-B

TPWD Does Not Have Processes to Identify All Data Processing Equipment with a Storage Device, including Printers, Copiers, Servers, or Fax Machines

In addition to desktop and laptop computers, TPWD surpluses printers, copiers, servers, and fax machines, some of which may contain a storage device. TPWD transfers these types of equipment to the Texas Facilities Commission's State Surplus storefront, which makes the equipment available for sale to the public. Auditors conducted an Internet search on the surplused printers available at TPWD to determine whether the equipment may contain a storage device (there were no copiers, servers, or fax machines available during testing).

Internet sources indicated that 3 (33.3 percent) of 9 printers designated to be transferred to the Texas Facilities Commission that auditors reviewed may contain a storage device. Auditors did not test those three printers to determine whether they actually contained a storage device. TPWD does not have policies and procedures in place requiring employees to inspect printers, copiers, servers, or fax machines for storage devices. According to TPWD management, those types of equipment are not searched to identify, remove, and sanitize any possible internal storage devices.

Chapter 3-C

TPWD Does Not Document All Required Information for Salvage or Surplus State Data Processing Equipment

TPWD correctly recorded in the Comptroller's State Property Accounting system whether equipment was acquired by non-state entities for all 30 disposal forms tested.

In addition, the form that TPWD used to document the disposal of data processing equipment includes many but not all of the required elements in Title 1, Texas Administrative Code, Section 202.28. Specifically, TPWD documents:

- Include the date of disposal, description of salvage or surplus items, serial numbers, inventory numbers, and names and addresses of the organizations to which the equipment was transferred (if applicable).
- Do not include the process and sanitization tools used to remove the data or method of destruction. TPWD could not provide auditors documentation showing the sanitization tools or the destruction methods used because that information is not being recorded.

Recommendations

TPWD should:

- Verify that hard drives marked as sanitized have had all data properly removed.
- Develop and implement policies and procedures to inspect all data processing equipment, including printers, copiers, servers, and fax machines, to identify, remove, and sanitize all internal hard drives prior to the equipment being surplused.
- Document the process and sanitization tools it used to remove data from salvage or surplus data processing equipment or the methods used to destroy the equipment.

Management's Response

Recommendation: *Verify that hard drives marked as sanitized have had all data properly removed.*

Management Response: We agree with this recommendation. We have modified our surplus tracking spreadsheet to include a section to verify that the hard drive has been physically removed from the computer. Removed hard drives are labeled with tracking information and typically stored by the analyst for a month in case data is needed by the end user. After a month, hard drives are transferred to the "non-wiped" hard drive bin for sanitation. We have also designated an area with plastic bins that will contain "non-wiped" drives and "wiped" drives needing verification. Wiped drives will still get an "E" marked on them with permanent marker indicating they've gone through the sanitation process. Once the drives have been verified that all data has been wiped, they will be transferred to the bin used to store drives prior to surplus pickup. We intend to have this implemented by the end of July 2011.

Responsible Party: TPWD Desktop Computing Services Manager.

Implementation Date: July 31, 2011

Recommendation: *Develop and implement policies and procedures to inspect all data processing equipment, including printers, copiers, servers, and fax machines, to identify, remove, and sanitize all internal hard drives prior to the equipment being surplused.*

Management Response: We agree with this recommendation. IT has worked out a procedure with the TPWD Surplus Property Manager who will contact IT when he receives printers or any other data processing equipment that could possibly contain hard drives. Desktop Support analysts will evaluate the printer and physically remove the hard drive and destroy it. We are also going to work with our providers of leased equipment to ensure that we are familiar with the procedure for purging these devices of data before they are returned to the vendor. We have already put this process into place.

Responsible Party: TPWD Desktop Computing Services Manager.

Implementation Date: Implemented.

Recommendation: *Document the process and sanitization tools it used to remove data from salvage or surplus data processing equipment or the methods used to destroy the equipment.*

Management Response: We agree with this recommendation. IT staff are documenting the new procedures and will disseminate them to all IT staff and management so that they are familiar with the new processes. We will have this completed by July 1, 2011.

Responsible Party: TPWD Desktop Computing Services Manager.

Implementation Date: July 1, 2011.

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Texas Department of Criminal Justice's (TDCJ) Computer Recovery Program (Program) and selected state entities remove or destroy data from electronic storage devices prior to the devices' sale, transfer, or destruction in accordance with state law, administrative rules, and state entity policies and procedures.

Scope

The scope of this audit covered the available inventory of data processing equipment at TDCJ and the inventory of data processing equipment that was available for transfer to other state entities or for sale to the public at the Texas Commission on Environmental Quality (TCEQ) and the Texas Parks and Wildlife Department (TPWD). The audit's scope also covered financial information related to the Program for fiscal years 2008 through 2010.

Methodology

The audit methodology included reviewing applicable laws, regulations, and guidelines; reviewing internal policies and procedures; interviewing key program personnel; testing hard drives from data processing equipment; and reviewing selected documentation.

To assess the reliability of the TDCJ's financial information for fiscal year 2010, auditors reviewed the systems that produced the information and interviewed personnel knowledgeable about the systems. Auditors also tested user access to and key application controls over the systems, as well as testing the data for completeness. Auditors determined that the data was sufficiently reliable for the purposes of this report.

Auditors also relied on prior audit work the State Auditor's Office conducted to assess the reliability of the State Property Accounting system (SPA). Auditors determined that SPA data was sufficiently reliable for the purposes of this audit.

<u>Information collected and reviewed</u> included the following:

- Statutes, regulations, and policies and procedures relevant to the audit objective.

- Guidelines, research, and common practices related to data sanitization.
- TDCJ internal audit report.
- TDCJ financial information related to the Program for fiscal years 2008 through 2010.
- TDCJ documentation for shipments of equipment from state agencies and institutions of higher education (state entities), school districts, and other political subdivisions.
- TDCJ documentation for the inspection of rebuilt or refurbished equipment.
- State Property Accounting system information related to TDCJ's assets and the equipment transferred from state entities to TDCJ.
- State Property Accounting system information related to the data processing equipment disposed as surplus by TCEQ and TPWD.
- Information from TCEQ's internal inventory system related to surplus data processing equipment.
- Documentation related to the surplus of data processing equipment at TCEQ and TPWD.

Procedures and tests conducted included the following:

- Sampled and tested hard drives that TDCJ received from state entities and school districts to determine whether the entities sent equipment to TDCJ that contained confidential or otherwise sensitive data.
- Sampled and tested hard drives in TDCJ's available inventory to determine whether the hard drives had been properly sanitized.
- Sampled and tested hard drives that TDCJ intended to sell as scrap material to determine whether the hard drives were operational, allowed information to be retrieved, and contained confidential or otherwise sensitive data.
- Sampled pallets of equipment that TDCJ received and compared the pallet contents to the shipping documentation that the transferring state entities and school districts prepared to determine whether all equipment with storage devices sent by the state entities and school districts arrived at TDCJ facilities.

- Conducted interviews with TDCJ, TCEQ, and TPWD personnel and reviewed the equipment used to wipe hard drives to determine whether the sanitization process was effective.

- Reviewed controls in place at TDCJ to determine whether there is a risk that data processing equipment may be stolen while in TDCJ’s custody.

- Sampled shipping documentation to determine whether the state entities transferring equipment to TDCJ completed the documentation in a consistent manner.

- Observed TDCJ physical search procedures to determine whether controls exist to maintain security over delivered goods.

- Conducted interviews and observed procedures to determine whether controls exist to ensure the security of equipment in transit to TDCJ.

- Reviewed TDCJ financial information related to the Program for fiscal years 2008 through 2010 to determine whether TDCJ was defraying the costs of its operations.

- Reviewed inventory of non-desktop and non-laptop equipment, such as copiers, printers, scanners, and personal digital assistants, at TDCJ, TCEQ, and TPWD to determine whether any of the equipment contained storage devices.

- Sampled hard drives from equipment at TCEQ and TPWD that were available for transfer to non-state entities to determine whether the equipment had been sanitized.

- Sampled documentation from TCEQ and TPWD related to surplus data processing equipment to determine whether the documentation complied with the relevant laws, regulations, and agency policies and procedures.

Criteria used included the following:

- Title 1, Texas Administrative Code, Section 202.28 (Removal of Data from Data Processing Equipment).

- Texas Government Code, Sections 403.272 and 403.278 (Responsibility for Property Accounting and Transfer of Personal Property).

- Texas Government Code, Section 497.012 (Repair and Resale of Surplus Data Processing Equipment).

- Texas Government Code, Section 2054.130 (Removal of Data from Data Processing Equipment).

- Texas Government Code, Sections 2175.125, 2175.128, and 2175.184 (Direct Transfer and Disposition of Data Processing Equipment).

- *Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology*, Special Publication 800-88, U.S. Department of Commerce, September 2006.

- Clearing and Sanitization Matrix, *The National Industrial Security Program Operating Manual*, U.S. Department of Defense Manual 5220.22-M, issued January 1995.

- *The National Industrial Security Program Operating Manual*, U.S. Department of Defense Manual 5220.22-M, reissued February 28, 2006.

- TDCJ's manufacturing and logistics standard operating procedures, 2010.

- TCEQ's *Guide for Administrative Procedures Manual*.

- TPWD policies and procedures for surplus and salvage property.

- Office of the Comptroller of Public Accounts' *State Property Accounting Process User's Guide*.

Project Information

Audit fieldwork was conducted from March 2011 through April 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The following members of the State Auditor's staff performed the audit:

- Arby J. Gonzales, CFE (Project Manager)

- Tony White, CFE (Assistant Project Manager)

- George Eure, MPA

- Justin Griffin, CISA

- Joseph K. Mungai, CIA, CISA

- Brenda Zamarripa

- Michelle Ann Duncan Feller, CPA, CIA (Quality Control Reviewer)

- Sandra Vice, CIA, CGAP, CISA (Assistant State Auditor)

Appendix 2

Figures Related to TDCJ's Computer Recovery Program

Tables 6 and 7 provide additional information about the Texas Department of Criminal Justice's (TDCJ) Computer Recovery Program (Program).

Table 6 lists the top 10 state agencies and higher education institutions (state entities) that used the Program to dispose of data processing equipment during fiscal years 2008 through 2010.

Table 6

Top 10 State Entities That Disposed of Data Processing Equipment Using the Program
Fiscal Years 2008 though 2010

State Entity	Number of Items Disposed
The University of Texas at Austin	13,721
The University of Texas M.D. Anderson Cancer Center	10,234
University of North Texas	7,826
Texas A&M University	6,683
The University of Texas Southwestern Medical Center at Dallas	5,628
Texas Department of Criminal Justice	5,601
The University of Texas at San Antonio	5,005
Texas State University - San Marcos	4,437
The University of Texas Health Science Center at Houston	4,326
Texas Tech University	4,284
Subtotal for the Top 10 State Entities	**67,745**
Subtotal for All Other State Entities	**60,366**
Total for All State Entities	**128,111**

Source: Office of the Comptroller of Public Accounts' (Comptroller) State Property Accounting system.

Table 7 lists the total number of data processing items disposed by state entities between fiscal years 2008 through 2010. This list includes both items state entities disposed of through TDCJ and items that state entities disposed of on their own.

Table 7

Items of Data Processing Equipment Disposed of by State Entities
Fiscal Years 2008 through 2010

Type of Equipment	Fiscal Year 2008	Fiscal Year 2009	Fiscal Year 2010	Total
Desktop Computer	52,018	43,979	43,049	139,046
Printer, Copier, Scanner, Fax Machine, Personal Digital Assistant	8,927	7,850	8,023	24,800
Laptop Computer	6,339	8,913	8,892	24,144
Server	1,043	1,344	1,437	3,824
Totals	**68,327**	**62,086**	**61,401**	**191,814**

Source: Comptroller's State Property Accounting system.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Joe Straus III, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas “Tommy” Williams, Member, Texas Senate
The Honorable Jim Pitts, House Appropriations Committee
The Honorable Harvey Hilderbran, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Texas Department of Criminal Justice

Members of the Texas Department of Criminal Justice Board
- Mr. Oliver J. Bell, Chairman
- Mr. Tom Mechler, Vice Chairman
- Mr. Leopoldo “Leo” Vasquez, III
- Mr. John “Eric” Gambrell
- Mr. Lawrence Gist
- Ms. Carmen Villanueva-Hiles
- Ms. Janice Harris Lord
- Mr. R. Terrell McCombs
- Mr. J. David Nelson

Mr. Brad Livingston, Executive Director

Texas Commission on Environmental Quality

Members of the Texas Commission on Environmental Quality
- Dr. Bryan W. Shaw, Chairman
- Mr. Buddy Garcia
- Mr. Carlos Rubinstein

Mr. Mark R. Vickery, P.G., Executive Director

Texas Parks and Wildlife Department

Members of the Texas Parks and Wildlife Commission
- Mr. Peter M. Holt, Chairman
- Mr. T. Dan Friedkin, Vice Chairman
- Mr. Ralph H. Duggins
- Dr. Antonio Falcon
- Ms. Karen J. Hixon
- Mr. Dan Allen Hughes, Jr.
- Ms. Margaret Martin
- Mr. S. Reed Morian
- Mr. Richard R. Scott
- Mr. Lee Marshall Bass, Chairman-Emeritus

Mr. Carter Smith, Executive Director