An Audit Report on the

Criminal Justice Division of the Office of the Governor

August 2002

Report No. 02-066

State
Auditor's
Office

An Audit Report on the

Criminal Justice Division of the Office of the Governor

SAO Report No. 02-066
August 2002

Overall Conclusion

The Criminal Justice Division of the Office of the Governor (Division) does not ensure that its grant recipients spend funds appropriately. The Division and its grantees could not provide evidence to support the appropriateness of an estimated $15.6 million in reimbursements. It also reimbursed certain grantees for unallowable expenditures. Furthermore, the Division cannot ensure the security, accuracy, or integrity of the data in its information systems that track grantee activity and Division expenditures. In fiscal year 2001, the Division made payments on 2,655 individual contracts and spent $150 million on its criminal justice programs.

Background Information

The Office of the Governor's Criminal Justice Division provides funding to local, regional, and statewide projects with the central goal of making Texas a safer state. The Division supports programs that promote help and healing for crime victims, provide safe places and positive role models for young Texans, and expand training opportunities for Texas law enforcement officers.

The Division administers funding from a variety of sources for a variety of purposes. These purposes include improvements in the areas of crime prevention, juvenile justice, and law enforcement.

In fiscal year 2001, the Division was appropriated $24 million in state funds and $63.8 million in federal funds. The Division also has the authority to carry forward unexpended balances from previous years, which is why it was able to spend $150 million in fiscal year 2001.

Key Points

The Division's Monitoring Procedures Do Not Ensure That Grantees Spend Funds Appropriately

The Division cannot rely on its current monitoring process to provide assurance that grantees are spending funds as intended. The purpose of the monitoring function is to ensure that grantees are reimbursed only for allowable expenditures. We requested support directly from grantees for expenditures that were reimbursed, but grantees could not always provide it. For fiscal year 2001, we estimate that as much as $15.6 million in reimbursements are in question because grantees could not provide the requested support.

Weaknesses in monitoring included inadequate guidelines on what monitors should review, insufficient documentation of monitoring results, and the practice of not monitoring grantees as scheduled. Of all monitoring files tested, 94 percent (49 of 52) did not contain sufficient support or documentation that would allow us to discern how monitors tested grantees' expenditures for appropriateness or made their assessments during the monitoring review. Furthermore, the Division does not have accurate data needed to effectively monitor grantees and reimburse only eligible expenses.

State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

This audit was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0133.

For more information regarding this report, contact Sandra Vice, Audit Manager, at (512) 936-9500.

The Division Does Not Ensure the Accuracy, Security, or Integrity of Data in Its Information Systems

Data in the Division's Grant Tracking System (GTS) and Financial Information System (FIS) are not always accurate, secure, or reliable. GTS does not have electronic edit checks to prevent users from deleting data in certain critical fields. GTS also does not have electronic edit checks to detect and correct user errors in a timely manner. Both GTS and FIS are at risk for unauthorized access because of inadequate procedures over the user IDs and passwords used to access the systems. Neither system adequately tracks changes made to system data. Furthermore, GTS does not have a complete definition of the data fields and what they should contain.

Summary of Information Technology Work Performed

We determined, as mentioned above, that the Division's information systems are at risk for unauthorized access and that the reliability of the data in the systems is at risk due to the lack of adequate edit checks and tracking mechanisms to ensure complete and accurate system data. Because of these weaknesses, grants could be awarded and paid fraudulently without detection. See Chapter 2 of this report for additional information.

GTS was implemented in March 2000 to allow the Division to track grant applications and their status. It also tracks awarded grants and related budget information, which included 2,655 individual grant contracts for which payments were made in fiscal year 2001. FIS is the system that houses all financial data related to payments, which totaled $150 million, made to the Division's grantees in fiscal year 2001. The information in FIS is periodically uploaded to the Uniform Statewide Accounting System. We conducted a limited review of GTS and FIS because they are the two major systems used to manage criminal justice grant activity. We did not test controls over external access into the Division's local network.

Summary of Management's Response

The Division disagrees with some of our findings but has agreed to implement all recommendations. The Division's responses are summarized in the Table of Results, Recommendations, and Responses that follows and also appear in full in Chapter 3 of this report (page 13).

Summary of Audit Objective, Scope, and Methodology

The objective of the audit was to determine whether the Criminal Justice Division of the Governor's Office manages the grant process to ensure that funds are spent in accordance with state and federal requirements and that internal agency procedures are applied consistently.

The scope of the audit included all Division grants and related expenditures reimbursed during fiscal year 2001.

Our methodology consisted of testing the Division's procedures over the needs assessment, the grant award, payments to grantees, and the monitoring processes. Additionally, we tested the grant award process followed locally by the Councils of Governments. We examined the accuracy and security of the major information systems that are used to process financial and contractual data at the Division.

Table of Results, Recommendations, and Responses [a]

Results and Recommendations 💻 denotes entry is related to Information Technology	Management's Response
The Division does not ensure that grantees maintain support for their expenditures. As a result, questioned expenditures are at least $15.6 million. (Page 1)	Disagree
The Division should:	
• Ensure that grantees maintain adequate documentation to support requests for funds. This documentation should support expenditures incurred during the specified request period.	Agree
• Increase training of Division monitors to allow for better detection of unallowable and/or unsupported expenditures.	Agree
• Maintain documentation to support contractual and equipment purchases as required by Division procedures.	Agree
The Division does not adequately monitor grantees, which puts money provided to grantees in fiscal year 2001 at risk of being misspent. (Page 3)	Disagree
The Division should ensure that:	
• Monitors are provided with detailed instructions on how to complete and support assessments made while utilizing the standard checklists.	Agree
• The monitoring review instruments and related policies and procedures are adequately and completely documented and that monitoring files contain evidence of test work performed, including the sampling methodology and actual test results from the review of documents such as invoices, travel vouchers, and receipts.	Agree
• Monitoring reviews occur as scheduled in the Division's risk assessment unless subsequent documented issues warrant a change.	Agree
• Grantees submit required documentation in a timely manner to ensure compliance with single audit requirements.	Agree
• All grantees subject to single audit requirements are appropriately tracked and monitored.	Agree
Insufficient or unreliable data limits the Division's ability to monitor and restrict payment to ineligible grantees. (Page 5)	Partially Agree
The Division should ensure the accuracy and completeness of all data that are used for tracking monitoring efforts and for placing grantees on vendor hold. The Division should also formalize procedures on how the vendor hold list is to be used and tracked.	Agree
💻 GTS and FIS lack adequate access controls. As a result, there is an increased risk that an unauthorized user could manipulate the data in the systems. (Page 7)	Partially Agree
The Division should make the following changes to GTS and FIS:	
• Remove generic user IDs.	Agree
• Set the systems to prompt users to change their passwords at least every 90 days.	Agree
• Enforce use of difficult-to-guess passwords with a mix of letters and numbers.	Agree
• Store passwords in an encrypted format.	Agree

[a] This table was completed by the management of the Criminal Justice Division. The Criminal Justice Division did not always agree with our findings (see shaded areas) but agreed to implement our recommendations.

Table of Results, Recommendations, and Responses [a]

Results and Recommendations 💻 denotes entry is related to Information Technology	Management's Response
💻 GTS does not ensure referential or data integrity. Therefore, Division staff do not have complete and reliable electronic information with which to make decisions. (Page 8)	Partially Agree
The Division should develop and implement system edits that will:	
• Prevent data from being deleted from the master table of GTS.	Agree
• Archive and close out a grant record as of a date specified by management. Management should also consider which procedures are best for the Division in defining the proper individuals who should have access to override the close-out date in the event that changes are needed.	Agree
• Identify user errors to increase the accuracy of GTS data.	Agree
💻 GTS and FIS do not completely track changes made to system data. The lack of adequate tracking of system changes increases the risk that changes to system data are not authorized by management. (Page 10)	Agree
The Division should:	
• Develop and execute audit logs in GTS and FIS that will track every addition, deletion, and modification of sensitive information in these systems.	Agree
• Review these logs regularly to ensure proper remedial action can be taken in case a user performs an unauthorized action.	Agree
💻 GTS does not have a complete data dictionary. Without one, it may be difficult to identify which of the 947 data fields contain relevant information. (Page 11)	Agree
The Division should ensure that its contractors develop a complete data dictionary for GTS. Management could use the data dictionary to assist in determining the critical information that should be tracked in the system and in cleaning out extraneous information.	Agree

Recent SAO Audit Work

Number	Report Name	Release Date
02-049	An Audit Report on Funds Collected as Court Costs	May 2002
02-345	State of Texas Federal Portion of the Statewide Single Audit Report for the Year Ended August 31, 2001	May 2002
01-555	The 2000 Statewide Single Audit Report	April 2001

[a] This table was completed by the management of the Criminal Justice Division. The Criminal Justice Division did not always agree with our findings (see shaded areas) but agreed to implement our recommendations.

Contents

Detailed Results

Appendix

Detailed Results

Chapter 1

The Division Does Not Ensure That Grantees Spend Funds Appropriately

The Criminal Justice Division of the Office of the Governor (Division) cannot rely on its current monitoring process to provide assurance that grantees are spending funds as intended. The purpose of the Division's monitoring function is to ensure that grantees are reimbursed only for allowable expenditures. We requested support directly from grantees for expenditures that were reimbursed, but grantees could not always provide it. For fiscal year 2001, we estimate that as much as $15.6 million in reimbursements are in question because grantees could not provide the requested support.

Criminal Justice Division Funds Audited—Fiscal Year 2001

State Funds (Appropriated Amount)

Criminal Justice Planning Fund	$23,600,000
Crime Stoppers Assistance Fund	$470,000

Federal Funds (Expended Amount)

Victims of Crime Act	$27,938,991
Safe and Drug Free Schools	$7,851,212
Juvenile Justice Delinquency Prevention	$5,973,525
Rural Domestic Violence	$459,414
Texas Narcotics Control Program	$30,880,652
Violence Against Women Act	$8,292,868
Juvenile Accountability Incentive Block	$11,712,172
Residential Substance Abuse Treatment	$5,727,815
Title V-Delinquency Prevention Program	$1,680,640

Source: Annual Financial Report 2001

Weaknesses in monitoring included inadequate guidelines on what monitors should review, insufficient documentation of monitoring results, and the practice of not monitoring grantees as scheduled. Of all monitoring files tested, 94 percent (49 of 52) did not contain sufficient support or documentation that would allow us to discern how monitors tested grantees' expenditures for appropriateness or made their assessments during the monitoring review.

Furthermore, the Division does not have accurate data needed to effectively monitor grantees and to reimburse only eligible grantees.

Chapter 1.1

The Division Does Not Ensure That Grantees Maintain Support for Their Expenditures

Because of inadequate processes, the Division cannot provide assurance that grantees were correctly reimbursed. For approximately 17 percent of the expenditure transactions tested (15 out of 90), grantees were unable to provide adequate support for the amount reimbursed by the Division. The expenditures in question total $113,497. Extrapolated to the total population of $150 million for fiscal year 2001, the projected amount of questioned expenditures is at least $15.6 million.

The Division bypassed a safeguard that would prevent it from reimbursing grantees for the same expense requested in multiple periods, or double-billing. The safeguard is that the grantee is required to identify on the request form a specific time frame during which expenditures have occurred or are expected to occur. In 11 of the 15 files with errors, grantees requested reimbursement to cover actual or anticipated expenditures, but the support provided did not match the time period claimed on the request. The Division asserts that it approves payment for any expenditures that occur within the entire grant period despite the procedures that are in place. Because the Division does not require grantees to submit support for expenses in most cases and cannot rely on its monitoring function to identify unallowable expenses, funds are at risk for being reimbursed more than once.

Our testing of expenditure transactions also showed that certain grantees were reimbursed for unallowable expenses and, in some cases, auditors were unable to determine the allowability of expenses from the approved grantee budget. One grantee received reimbursement for supplies even though the only allowable budgeted expenditure was for salary expenses. This grantee received an on-site monitoring review by the Division in fiscal year 2001. However, the monitors did not identify this issue. Another grantee was reimbursed for membership dues, which was also an unallowable expenditure. Once we notified the Division of the issue, the Division requested that the grantee reimburse the unallowable membership fees.

Additionally, in some of the expenditure files tested, the Division reimbursed grantees for unverified contractual or equipment expenses although the grantees did not provide required documentation directly to the Division to support these expenses at the time the funds were requested. The Division's procedures require that grantees attach invoices to their requests for funds if they are requesting reimbursement for purchased services or equipment. The Division paid these expenses without knowing whether they were appropriate and legitimate expenditures. For example, one grantee was reimbursed $18,841 for contractual services. The Division did not have documentation to verify that the grantee submitted supporting invoices with the original request.

Recommendations

The Division should:

- Ensure that grantees maintain adequate documentation to support requests for funds. This documentation should support expenditures incurred during the specified request period.
- Increase training of Division monitors to allow for better detection of unallowable and/or unsupported expenditures.
- Maintain documentation to support contractual and equipment purchases as required by Division procedures.

Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

Chapter 1.2

The Division Does Not Adequately Monitor Grantees

The Division's inadequate monitoring procedures put money provided to grantees in fiscal year 2001 at risk of being misspent. The Division relies on the Quality Assurance Division to ensure that grantees are reimbursed for allowable expenses. The Division has a contractor that performs annual desk reviews and/or on-site visits of grantees.

A review of monitoring procedures and testing of a statistical sample of grantees revealed three issues:

Deviation from monitoring schedule. Of the grantees we tested, the Division did not monitor 38 of the grantees as they were scheduled on its risk assessment. Two additional grantees received desk reviews even though the risk assessment showed that they were scheduled to receive a more intensive on-site review. There was no documentation to explain why the monitoring schedule was not followed. The Division relies on monitors to ensure that grantees are reimbursed for allowable expenditures after reimbursements have been made. Therefore, it is important that the Division monitor its grantees in accordance with its risk assessment unless subsequent documented factors warrant a change.

Inadequate monitoring guidelines and insufficient documentation of reviews. The Division does not have guidelines in place detailing how monitors should use the standard monitoring checklists or stating what documentation monitors need to support their results. For example, 49 of the 52 monitoring files tested did not include proper documentation, such as tests performed or sampling methodology used, to support the monitoring result. Without documented monitoring guidelines, there is no assurance that monitors will review grantees accurately or consistently.

Furthermore, 4 of the 49 grantees mentioned above did not have files detailing their monitoring visits or checklists, which is the standard monitoring review instrument. Without these on file, there is no assurance that all grantees were monitored in accordance with the Division's risk assessment schedule.

Single Audit Requirements

OMB Circular A-133

1. Non-Federal entities that expend $300,000 or more in Federal funds (from all sources including pass-through subawards) in the organization fiscal year (12 month turnaround reporting period) shall have a single organization-wide audit conducted in accordance with the provisions of *OMB Circular A-133*.
2. Non-Federal entities that expend less than $300,000 a year in Federal awards are exempt from Federal audit requirements for that year. Records must be available for review or audit by appropriate officials including the Federal agency, pass-through entity, and General Accounting Office.

Audits are due no later than nine (9) months after the close of each fiscal year during the term of the award.

Inadequate assurance of grantee compliance with single audit requirements. The Division cannot ensure that its grantees have complied with single audit requirements (see text box). During our audit, we identified 16 grantees whose compliance with single audit requirements was in question:

- Five grantees did not submit their single audit reports to the Division within nine months of their fiscal-year end as required by *OMB Circular A-133*.

- For nine grantee files, auditors could not determine whether the single audit requirements applied. According to *OMB Circular A-133*, if a grantee certifies that it spent $300,000 or more in federal or state funds from all funding sources, the grantee is required to receive a single audit review from an independent audit function. The Division requires grantees to submit certification forms indicating the amount of federal and/or state funds expended. This certification from the grantees was not in the nine files.

- Two of the grantees tested were required to submit single audit reports to the Division. However, the two grantees did not submit single audit reports to the Division for fiscal year 2001. The total questionable costs related to these two grantees for fiscal year 2000 is $115,686.

Recommendations

The Division should ensure that:

- Monitors are provided with detailed instructions on how to complete and support assessments made while utilizing the standard checklists.

- The monitoring review instruments and related policies and procedures are adequately and completely documented and that monitoring files contain evidence of test work performed, including the sampling methodology and actual test results from the review of documents such as invoices, travel vouchers, and receipts.

- Monitoring reviews occur as scheduled in the Division's risk assessment unless subsequent documented issues warrant a change.

- Grantees submit required documentation in a timely manner to ensure compliance with single audit requirements.

- All grantees subject to single audit requirements are appropriately tracked and monitored.

Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

Chapter 1.3

Insufficient or Unreliable Data Limits the Division's Ability to Monitor and Restrict Payment to Ineligible Grantees

The Division does not accurately maintain certain data relevant to ensuring effective monitoring of grantees. We identified several instances in which data critical for monitoring were inaccurate or not available in the Division's tracking systems:

- In several instances, grantees were not included in the risk assessment for fiscal year 2001. The data for the risk assessment are obtained from a report that lists all active grantees, and according to the Division's procedures, the risk assessment should have covered all grantees that were active in fiscal year 2001.

- There were also instances in which the scheduled monitoring date recorded in the tracking tools did not match the date of the actual visit on the review instrument/checklist.

Additionally, the Division's vendor hold list does not provide complete and accurate information that will allow staff to effectively stop payments to grantees when needed. The Division's Financial Information System (FIS), which processes payments, contains a list of grantees that have been placed on vendor hold. Accounting staff members also maintain a version of the vendor hold list in a separate spreadsheet. Grantees that have been placed on vendor hold are unable to receive payment until they take care of the issues that caused the Division to put them on hold. For example, a grantee may owe the Division a refund because the Division previously overpaid the grantee. The grantee is placed on vendor hold until the Division receives the refund.

We noted several discrepancies between the vendor hold list maintained in FIS and the one maintained by the accounting staff. As of August 30, 2001, five grantees on the spreadsheet version of the vendor hold list were not included in the FIS version. Two grantees listed as inactive on the FIS version were listed as active on the spreadsheet version. There were three grantees that appeared on the FIS version but that were not included on the hard copy version of the vendor hold list. Because grantees on the vendor hold list should not receive payments from the Division, it is important that the list be accurate and complete in both versions.

Recommendation

The Division should ensure the accuracy and completeness of all data that are used for tracking monitoring efforts and for placing grantees on vendor hold. The Division should also formalize how the vendor hold list is to be used and tracked.

Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

This page intentionally left blank.

Chapter 2

The Division Does Not Ensure the Accuracy, Security, or Integrity of Data in Its Information Systems

Data in the Division's Grant Tracking System (GTS) and Financial Information System (FIS) are not always accurate, secure, or reliable. Because of these weaknesses, grants could be awarded and paid fraudulently without detection. GTS does not have electronic edit checks to prevent users from deleting data in certain critical fields. GTS also does not have electronic edit checks to detect and correct user errors in a timely manner. Both GTS and FIS are at risk for unauthorized access because of inadequate procedures over the user IDs and passwords used to access the systems. Unauthorized access could result in data manipulation and/or loss of funds due to fraud. Neither system adequately tracks changes made to system data. Furthermore, GTS does not have a complete definition of the data fields and what they should contain.

The Division uses these two systems to manage criminal justice grant activity. GTS was implemented in March 2000 to allow the Division to track grant applications and their status. It also tracks awarded grants and related budget information. FIS houses all financial data that relate to payments made to the Division's grantees. The information in FIS is periodically uploaded to the Uniform Statewide Accounting System. The Division made payments on 2,655 individual contracts and expended a total of $150 million in fiscal year 2001.

Chapter 2.1

GTS and FIS Lack Adequate Access Controls

The Division has not used the security features of user IDs and passwords effectively to protect the data in GTS and FIS. As a result, there is an increased risk that an unauthorized user could manipulate the data in the systems. Specifically:

- Both systems allow the use of generic user IDs. GTS has 17 active generic user IDs. For example, Division interns use 9 of the 17 generic user IDs. In FIS, there is one generic user ID that is commonly used. Generic user IDs do not allow the Division to track who makes changes in the system, which may hinder accountability.

What Is a User ID and Why Is Using Generic User IDs a Problem?

The user ID is a unique identifier of an individual who has access to a system. Generic user IDs, because they are not user-specific, make it hard to ensure that only authorized individuals access the system. With generic user IDs, system use cannot easily be tracked to a specific individual.

- GTS does not require users to change their passwords regularly. Additionally, users are not required to change their passwords from the default or initial password setting. Of 77 GTS users, 49 had not changed their passwords from the passwords originally assigned to them when the system was executed in March 2000.

- Passwords for GTS and FIS are short and simple. Of the 77 GTS passwords, 27 were simple words or names that contained either all letters or all numbers. Only one password contained both letters and numbers. All of the 31 FIS users have unique passwords. However, 26 of the 31 passwords are simple ones containing either all letters or all numbers.

Additionally, the password tables in both of the systems are not encrypted. We requested a complete replica of the data in both systems and found that all passwords were clearly visible and were contained in one file in each of the replicas.

The lack of adequate access controls puts all the data in the GTS and FIS databases at risk for unauthorized access. It is considered both a good business practice and an industry standard to have users create their own difficult-to-guess passwords, to change passwords every 60 to 90 days, to store passwords in an encrypted format, and to assign unique user IDs. If an unauthorized user were to gain access to the systems, a false grantee account could be created and funds could be issued for that account.

Recommendations

The Division should make the following changes to the Grant Tracking System and the Financial Information System:

- Remove generic user IDs.
- Set the systems to prompt users to change their passwords at least every 90 days.
- Enforce use of difficult-to-guess passwords with a mix of letters and numbers.
- Store passwords in an encrypted format.

Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

Chapter 2.2

GTS Does Not Ensure Referential or Data Integrity

GTS does not have adequate electronic edit checks to ensure referential or data integrity (see text box). Without such edit checks, Division staff do not have complete and reliable electronic information with which to make decisions.

Referential integrity is a system feature that prevents users or applications from entering inconsistent data or changing data so that it is no longer consistent. For example, referential integrity would prevent a person from deleting a record if that record supplies information to other parts of the system.

Data integrity means that data contained in a system is accurate and complete.

Referential integrity. GTS does not

prevent users from deleting information from the master table when there are records associated with that information. As a result, some grantees' electronic files contain empty fields, which at a minimum prevents the Division from having a complete electronic history of the grants. However, the missing information also creates a risk that the Division may make payments to unauthorized individuals. Some grantees' records do not list the "authorized grant official" because that person's name may have been deleted from the master table. The authorized grant official is the individual designated by the grantee and approved by the Division to request reimbursement for incurred expenditures. The Division's accounting staff must validate that the person requesting reimbursement is the authorized official before processing a payment. Because GTS allows the contents of this field to be deleted or left blank, the Division is at risk for disbursing payments to unauthorized individuals.

Data integrity. GTS does not have an edit in place to archive and completely close out a grant record as of a specified date. Without this edit check, there is an increased risk that an unauthorized person could change grant information. Because changes are allowed, even on very old data, the changes are unlikely to be reviewed.

Furthermore, there is no automated process within GTS to identify user errors. One Division employee performs a cursory review of GTS-generated reports to look for errors. While this employee does identify errors, an automated process could help identify more errors.

Recommendations

To ensure referential and data integrity, the Division should develop and implement system edits that will:

- Prevent data from being deleted from the master table of GTS.
- Archive and close out a grant record as of a date specified by management. Management should also consider which procedures are best for the Division in defining the proper individuals who should have access that permits them to override the close-out date in the event that changes are needed.
- Identify user errors to increase the accuracy of GTS data.

Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

Chapter 2.3

GTS and FIS Do Not Adequately Track Changes Made to System Data

Neither GTS nor FIS creates an adequate access log detailing who changed data and when. FIS tracks some changes, but management does not review the log. The lack of adequate access logs and reviews increases the risk that changes to system data may not be authorized by management.

For example, GTS does not electronically track who clears special conditions for grants. A special condition occurs after a grant is awarded. Generally, the grantee must provide additional, sometimes critical, information to the Division before the accounting system will process payments. (For example, the Division may require a certified assurance of the grantee's financial status.) When the Division receives the required information, the special condition is cleared and the grantee is allowed to receive payment. Because GTS does not track who clears special conditions, there is an increased risk that an unauthorized person will clear the special condition. While there are manual processes in place for clearing special conditions, an electronic report that details the special conditions cleared over a specified period would allow management to quickly and easily identify changes to system data.

FIS's audit logs record only the person who created the original record and the person who made the last updates. Users who make any changes to the financial information in the interim cannot be identified. Furthermore, management does not review the information that is logged by FIS.

Best business practices dictate a regular review of complete audit logs, which deter improper behavior and provide accountability for all user actions. This is supported by experts in the field, such as Charles Cresson Wood, CISA, CISSP, an expert in information security. Wood recommends in his book *Information Security Policies Made Easy* that "All production application systems which handle sensitive information must generate logs that show every addition, modification and deletion to such sensitive information."

Recommendations

The Division should:

- Develop and execute audit logs in GTS and FIS that will track every addition, deletion, and modification of sensitive information in these systems.
- Review these logs regularly to ensure proper remedial action can be taken in case a user performs an unauthorized action.

Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

Chapter 2.4

GTS Does Not Have a Complete Data Dictionary

GTS does not have a data dictionary that clearly defines what information is contained in each of the 947 fields in the system. The Division provided the auditors with a data dictionary that listed only the field names and their properties (such as alpha or numeric and number of characters in each field) in the GTS database.

Without a data dictionary, it may be difficult to identify which fields contain relevant information. In the event that GTS's contract programmer stops working with the Division, a complete data dictionary will make it easier for a new programmer to understand what GTS contains. The Institute of Internal Auditors Research Foundation's *Systems Auditability and Control Report,* Module 5 (December 1991), states that "At the core of a data dictionary are metadata … which provide information describing the data and their meaning."

Recommendation

The Division should ensure that its contractors develop a complete data dictionary for GTS. Management could use the data dictionary to assist in determining the critical information that should be tracked in the system and in cleaning out extraneous information.

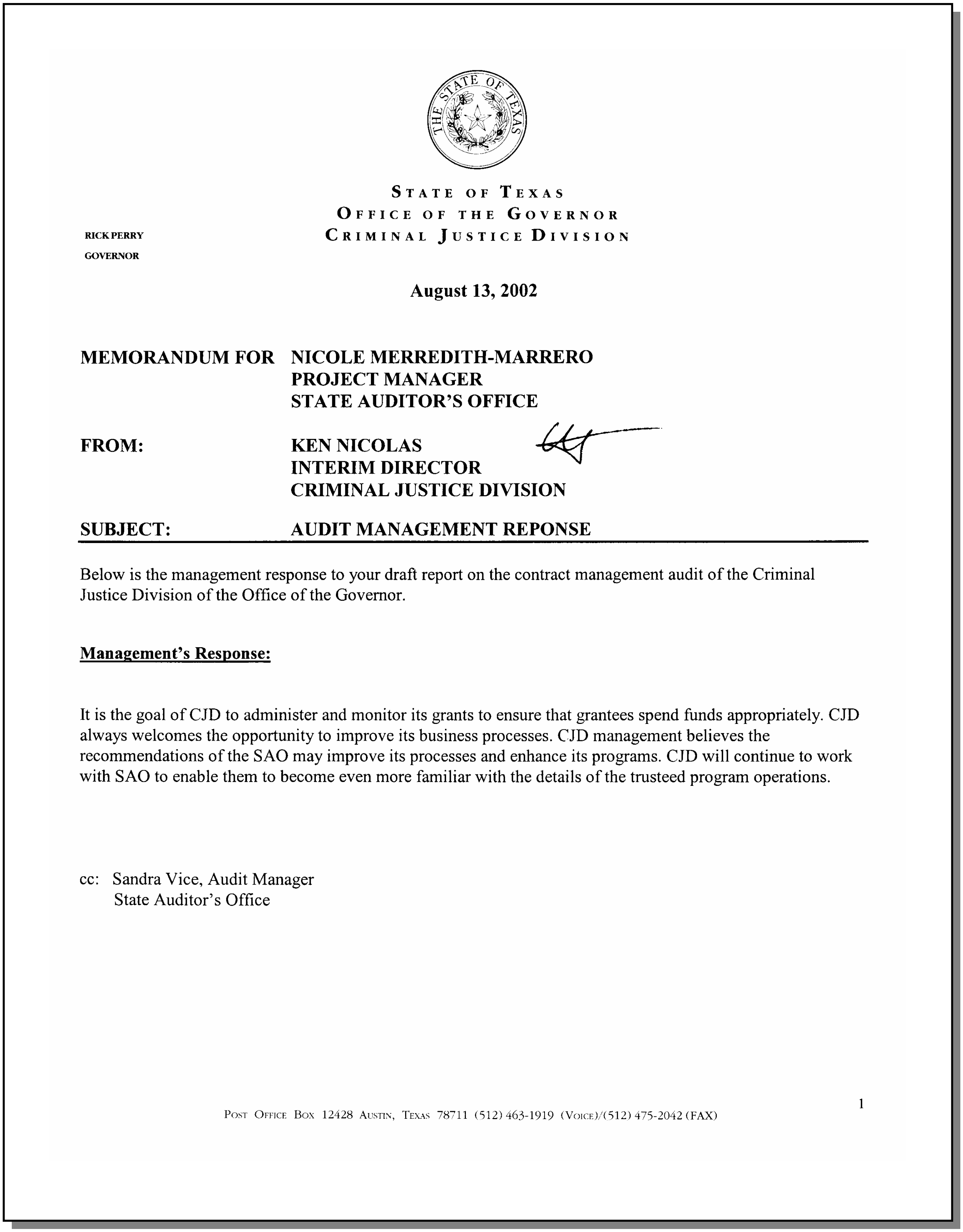
Management's Response

The Division's responses to all findings are summarized in the Table of Results, Recommendations, and Responses and appear in full in Chapter 3 of this report.

This page intentionally left blank.

Chapter 3

Management's Responses



STATE OF TEXAS
OFFICE OF THE GOVERNOR
CRIMINAL JUSTICE DIVISION

RICK PERRY
GOVERNOR

August 13, 2002

MEMORANDUM FOR NICOLE MERREDITH-MARRERO
PROJECT MANAGER
STATE AUDITOR'S OFFICE

FROM: KEN NICOLAS
INTERIM DIRECTOR
CRIMINAL JUSTICE DIVISION

SUBJECT: AUDIT MANAGEMENT REPONSE

Below is the management response to your draft report on the contract management audit of the Criminal Justice Division of the Office of the Governor.

Management's Response:

It is the goal of CJD to administer and monitor its grants to ensure that grantees spend funds appropriately. CJD always welcomes the opportunity to improve its business processes. CJD management believes the recommendations of the SAO may improve its processes and enhance its programs. CJD will continue to work with SAO to enable them to become even more familiar with the details of the trusteed program operations.

cc: Sandra Vice, Audit Manager
State Auditor's Office

1

POST OFFICE BOX 12428 AUSTIN, TEXAS 78711 (512) 463-1919 (VOICE)/(512) 475-2042 (FAX)

This page intentionally left blank.

Appendix

Objective, Scope, and Methodology

Objective

The objective of the audit was to determine whether the Criminal Justice Division of the Governor's Office (Division) manages the grant process to ensure that funds are spent in accordance with state and federal requirements and that internal agency procedures are applied consistently.

Scope

The scope of the audit included all grants and related expenditures reimbursed during fiscal year 2001. We reviewed local and statewide grants as well as grants from the Division to other state agencies. State funds tested were the Criminal Justice Planning Fund and the Crime Stoppers Assistance Fund. Federal funds tested included Victims of Crime Act, Safe and Drug Free Schools, Juvenile Justice Delinquency Prevention, Rural Domestic Violence, Texas Narcotics Control Program, Violence Against Women Act, Juvenile Accountability Incentive Block, Residential Substance Abuse Treatment, and Title V-Delinquency Prevention Program.

We tested the Division's procedures over the needs assessment, the grant award, payments to grantees, and the monitoring processes. Additionally, we tested the grant award process followed locally by the Councils of Governments. We examined the accuracy and security of the major information systems that are used to process financial and contractual data at the Division.

Methodology

The methodology used on this audit consisted of obtaining and reviewing procedures and data, conducting random sample tests, and analyzing and evaluating data and test results.

Information obtained, reviewed, tested, and analyzed included the following:

- Interviews with Criminal Justice Division management and staff.
- Documentary and analytical evidence such as:
  - Division policies and procedures.
  - Applicable state and federal statutes and guidelines.
  - Review of controls over critical grant and finance-related information systems.
  - Tests of 90 randomly selected grant and monitoring files.

  - Analysis of federal funds management.
  - *Information Security Policies Made Easy*, Version 7, Charles Cresson Wood, CISA, CISSP, October 1999.
  - *Systems Audibility and Control Report,* Module 5, The Institute of Internal Auditors Research Foundation, December 1991.

- We reviewed and tested the Division's policies and procedures used to:
  - Determine the needs of the state.
  - Select and award grants.
  - Monitor grantees.
  - Manage and protect its critical information systems.

We conducted fieldwork from January 2002 through June 2002. The audit was conducted in accordance with applicable professional standards, including generally accepted government auditing standards.

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

- Nicole J. Merridth-Marrero, MBA (Project Manager)
- Courtney Ambres-Wade (Assistant Project Manager)
- Adriana Buford, CPA, CIA (Assistant Project Manager)
- Lori A. Field
- Jennifer Hedrick
- Fred Bednarski
- Kelly Trish, MPAff, JD
- Bruce Truitt, MPA, MA
- Serra Tamur, MPA, CISA
- Dorvin Handrick, CISA, CDP
- J. Scott Killingsworth, CIA (Quality Control Reviewer)
- Sandra Vice, MPAff (Audit Manager)
- Frank Vito, CPA (Director)

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable James E. “Pete” Laney, Speaker of the House, Chair
The Honorable Bill Ratliff, Lieutenant Governor, Vice Chair
The Honorable Rodney Ellis, Senate Finance Committee
The Honorable Florence Shapiro, Senate State Affairs Committee
The Honorable Robert Junell, House Appropriations Committee
The Honorable Rene O. Oliveira, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor
Dr. Michael McKinney, Chief of Staff
Mr. Ken Nicolas, Interim Director, Criminal Justice Division

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact Production Services at (512) 936-9880 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government call the SAO Hotline: 1-800-TX-AUDIT.