

147375



United States
General Accounting Office
Washington, D.C. 20548

Accounting and Financial
Management Division

B-114839



147375

August 19, 1992

The Honorable Michael P. W. Stone
Chairman, Board of Directors
Panama Canal Commission

Dear Mr. Stone:

We have issued opinions on the financial statements of the Panama Canal Commission and on its internal control structure, and have reported on its compliance with applicable laws and regulations for the year ended September 30, 1991 (GAO/AFMD-92-69).

In planning and performing our audit on the financial statements of the Commission, we identified several matters regarding accounting procedures and internal control structure which could be improved. These include the need for timely closeouts of capital work requests; better segregation of duties for journal entries and the Marine Billing System; documentation of computer system methodology; and improved security through more frequent changes of security passwords, centralized responsibility over information assets, limited access to computer production programs, and restricted physical access to the Administration Building.

These matters are not material in relation to the financial statements, but nevertheless warrant the attention of management. The purpose of this letter is to advise you of these matters and our suggestions for their improvement. We discussed the matters addressed in this letter with Commission supervisory personnel responsible for the area and have included their comments for your information.

TIMELY CLOSINGS OF CAPITAL
WORK REQUESTS

Fixed assets are not being transferred on a timely basis from the Plant-Additions-In-Progress account to the appropriate completed plant account when the capital project is ready for its intended use. During our test of completed

GAO/AFMD-92-71ML

055174/147375

fiscal year 1991 capital work requests, we noted that 9 of 10 closings were recorded at least 8 months after they were ready for use. Five of these were recorded in the subsequent fiscal year after their effective service date. The internal control standards in GAO's Policy and Procedures Manual for Guidance of Federal Agencies require that transactions and other significant events be promptly recorded.

This condition is occurring because field units are not promptly sending completion notices, which is the basis for recording a closing entry, to the Plant-In-Progress Section. Additionally, personnel shortages in the Plant-In-Progress Section and the batching of completion notices by field units contribute to a backlog of unprocessed completion notices. The effect of not closing capital work requests in a timely manner is a delay in recording depreciation expense. Thus, depreciation expense is understated, and the book value of property, plant, and equipment is overstated. In addition, improper costs may be charged when work request job numbers remain open in the Job Control System for an extended period.

We suggest that the Plant-In-Progress Section more closely monitor projects near completion to ensure that field units send the completion notices as soon as the projects are completed. Comparing amounts authorized to amounts expended would be a technique for determining whether projects are approaching completion.

The Chief, General Ledger Branch, concurred with the above suggestion and stated that two changes are being made for fiscal year 1992 to assist in recording these entries on a more timely basis. First, for contracted projects, preliminary closings are now being made from the Use and Possession letters. These letters are sent to contractors by the Commission to inform them that the Commission is going to take possession of the asset, even though portions of the contract may not have been completed. The Chief estimated that in most cases when these letters are issued, the projects are at least 90 percent complete.

Secondly, a computer-generated report which details all costs incurred to date on a capital project is now being compared with the amounts authorized on the Capital Work Request form. Once project costs are substantially complete (e.g., 90 percent complete), the Plant-In-Progress Section

will query the appropriate field unit to determine if the project is ready to be placed into service at which time a closing entry would be prepared. It is our understanding that these procedures have significantly improved the timeliness of work request closings in fiscal year 1992.

SEGREGATION OF DUTIES

Journal Entry Approval Process

Supervisory personnel in the Accounting Division responsible for reviewing journal entries may make journal entries without a higher level of review. According to internal control standards in GAO's Policy and Procedures Manual for Guidance of Federal Agencies, the processing, recording, and reviewing of transactions should be separated.

This condition exists during critical processing periods to meet deadlines, such as during the month-end or year-end closing of the general ledger. This lack of control could allow unauthorized entries to be made into the system and not be detected.

Currently, each branch prepares a log of the journal entries which have been reviewed. This log identifies the preparer, the reviewer, a description of the journal entry, and the number of entry lines processed. We suggest that the Accounting Division require the Chiefs of each Branch to review the log of journal entries to ensure that the preparer was also not the reviewer and that the number of journal entry lines recorded in this log reconcile to the number of lines processed by Data Processing. This will help ensure the accountability of all journal entries and the corresponding review by supervisory personnel.

The Chief Accountant said he will require Branch Chiefs to review the logs and reconcile the number of lines processed to the number of lines for journal entries initiated in their area.

Marine Billing System

The Director of the Admeasurement Division, the Chief Admeasurer, and four supervisory admeasurers have unrestricted access to the Marine Billing System. This allows them to enter data from the tolls charge form, which includes source information for invoicing ships which transit the Canal, and to approve these data for billing.

This broad practice of allowing employees access to both enter and review billing information violates basic segregation of duty standards. Without adequate separation of duties, opportunities exist for these supervisory personnel to make unauthorized changes to tolls charge information without detection, increasing the risk that incorrect invoices could be processed.

We suggest that the Marine Billing System be modified to preclude supervisory admeasurement personnel from approving any tolls charge transaction that they entered.

The Director, Admeasurement Division, agreed that the Marine Billing System does not contain controls for adequate segregation of duties. A change was requested to the automated Marine Billing System which would prevent an individual who enters data from checking or approving those data. The Commission's Chief Financial Officer told us that this change was implemented in July 1992.

DOCUMENTATION OF
SYSTEM DEVELOPMENT METHODOLOGY

Key phases of the Financial Management Information Systems (FMIS) methodology used to develop and maintain application systems are not documented in the Data Processing System Manuals. Generally accepted data processing standards suggest that management issue a written policy statement to structure and control the process of developing computerized information systems. Without documentation for all phases of the system development life cycle and the tasks associated with each phase, the Commission cannot be assured that employees and managers will utilize procedures and controls necessary to develop and maintain adequate and well controlled financial applications.

According to system personnel, this condition is attributable to the intensive amount of time required to document each type of project. FMIS added a Quality Assurance Test Procedures Volume (Volume 07) to its Data Processing System Manuals in November 1991, but phases such as project initiation, feasibility studies, design, and tasks associated with these phases have not yet been addressed. Additionally, testing procedures for emergency changes made directly to production program libraries are not included in the Quality Assurance Test Procedures Volume.

We suggest that FMIS identify and describe all phases associated with developing and maintaining application systems in the Data Processing System Manuals and establish a time frame for completion of this documentation. We also suggest that testing procedures be added for emergency changes to production program libraries.

The Chief, FMIS, agreed to identify all phases of the system development life cycle which are not included in the Data Processing System Manuals during calendar year 1992. The Commission will begin incorporating these phases and the tasks associated with them in the Data Processing System Manuals. FMIS also agreed to add emergency testing procedures to the Quality Assurance Test Procedures Volume during calendar year 1992.

IMPROVED SECURITY

System Password Policy

User passwords for the Marine Traffic Control System (MTCS) have not been changed since at least August 1990. This system mainly contains ship, scheduling, and resource information concerning transits through the Canal. However, subsystems of MTCS such as the Ship Clearance Panels and the Marine Billing System are used to clear ships for transit through the Canal after certain financial conditions are met and to produce invoices for ship transits. Generally accepted data processing standards prescribe that access controls be established to protect computer resources against unauthorized use or modification, damage, or loss. Specifically, access to computer information should be restricted by the use of a password.

Although FMIS has begun to notify the security coordinators of the need to change passwords for their on-line applications, and most financial application passwords have been changed, MTCS has not complied with this notification. According to the Chief, FMIS, since there are many users of MTCS, the security coordinator has not wanted to change passwords because the cost involved in coordinating the password change and correcting problems caused by people forgetting their passwords is perceived to outweigh the risk involved in not changing the passwords. However, if passwords are not changed periodically, the risk of unauthorized access or modification to computer data is increased.

We suggest that FMIS exercise authority over password security and establish procedures to ensure that user passwords for all financially related on-line applications are changed at least annually.

The Chief, FMIS, agreed to control the passwords for the Marine Billing System and Ship Clearance Panels of the MTCS since these functions relate to the Commission's financial operations. He also agreed to change the security software settings to require users of the Marine Billing System and users with access to the Ship Clearance Panels to change their passwords every 6 months. Although our audit work did not specifically address the Time and Reporting System and the on-line portion of the Payroll System, FMIS also agreed to change the security settings to require users of these systems to change their passwords every 6 months. The Commission's Chief Financial Officer told us that these changes were implemented in June 1992.

Centralized Responsibility Over Information Assets

Responsibility for information security is fragmented throughout the Commission with no branch or division having overall responsibility for data and physical security of the Commission's information assets. Generally accepted data processing standards suggest that the responsibility for ensuring both the data and physical security of an organization's information assets should be assigned to an information security manager, reporting to the organization's senior management. This individual should not have any responsibility for programming, operating computer hardware, or entering data for processing by the information services department.

FMIS is responsible for information security controls including maintaining data security controls. However, FMIS has delegated the responsibility for controlling authorization of on-line computer access and changes to on-line user passwords to various application coordinators located in the user department which FMIS views as the "owner" of the application system. Without a security administrator to monitor overall security functions, the Commission has no assurance that its security policies are being uniformly followed or that its information assets are being adequately protected.

We suggest that the Office of Executive Administration designate an overall Security Administrator who reports to

senior Commission management and is responsible for ensuring both data and physical security over the information assets. The Security Administrator should

- issue an information security policy statement which requires that the Commission adequately secure its information assets, and clearly define the responsibilities of users, management, and security administrators in security matters, and
- oversee the functions of the application security coordinators and the FMIS security coordinator to ensure that appropriate security is established and maintained.

The Chief, Administrative Services Division, has agreed to designate a security administrator who does not have responsibility for programming, operating computer hardware, or entering data for processing. However, due to budget limitations, the Commission will probably not be able to implement this change until the beginning of fiscal year 1993.

Administration Building Security

Physical access to the Commission's Administration Building, where the Central Computer Facility is located, is not adequately secured and restricted. The Commission's security procedures require that guards verify the identity of persons entering a facility and, at their discretion, search bags. However, over an 8-day period, our computer specialist was stopped by the guards on only two occasions, once to sign the visitor's log and once to show proper Commission identification. The staff member's bag was never inspected. Furthermore, the parking lot adjacent to the wing of the Administration Building which houses the Central Computer Facility is open to unauthorized vehicles. Generally accepted data processing standards suggest that computers, information, and data are assets that should be managed properly and protected against theft, loss, unauthorized manipulation, fraudulent activities and natural disasters.

The current conditions increase the risk of unauthorized access or damage to the computer facility. Unless security procedures are consistently followed, opportunities exist to interrupt data center operations and the flow of data needed to effectively manage Canal operations.

Although the Commission has discussed increased security for the Administration Building, including limiting parking in Administration Building lots to Commission employees with windshield decals, at the time of our review no actions had been approved.

We suggest that

- the Canal Protection Division improve security over access to the Administration Building and monitor compliance with the required procedures for admitting people into the Administration Building and
- the Administrative Services Division designate the Administration Building parking lots as reserved "decal" parking for employees. This would allow the Canal Protection Guards to detect unauthorized vehicles during routine checks and, if necessary, control parking in these lots.

The Assistant Chief, Canal Protection Division, stated that he is continuing to explore possible enhancements to physical security over the Administration Building and will begin looking at improving security over access to the Management Information Systems wing. Additionally, the Administrative Services Division is planning to study the feasibility of making the parking area near the computer facility reserved "decal" parking for Commission employees.

Access To Computer Production Programs

The Data Processing Division allows supervisory systems analysts and senior systems analysts access to the computer production program libraries to perform emergency program changes. Production programs instruct the computer how to process and accumulate accounting information in the financial systems. Additionally, the systems analysts initiate the problem reports used to monitor and report access to the production program libraries. Generally accepted data processing standards provide that access to specified production programs should be granted based on an individual's need for such access and under a controlled environment in which periodic reviews of such access are performed.

Whenever a systems analyst performs emergency program changes, the analyst is to complete a Management Information System Application System Problem Report which is forwarded

for review. The problem report provides, among other information, a description of the program change, who made the program change, and when the program change was made. Although emergency program changes are required infrequently, systems analysts are always allowed access to on-line production libraries such as the Marine Traffic Control System and the Time Reporting System which are considered critical to the operations of the Canal. The Marine Traffic Control System regulates each ship's transit through the Canal and also produces invoices for tolls and other miscellaneous revenue collected from transiting vessels. The Time Reporting System captures and verifies timekeeping data that is passed to the Payroll System which performs the pay calculations and processes checks for the Commission's work force of about 9,000 employees.

This condition exists in order to avoid disruption of critical on-line system processing. However, with unrestricted access to production programs, supervisory systems analysts and senior systems analysts could insert, modify, or delete computer program instructions for the on-line systems and easily obtain detailed knowledge of the system to change programs that might result in unauthorized transactions.

We suggest that FMIS use features of its security software to create a report identifying instances when the production program libraries are accessed. This report should be reconciled to the log of emergency changes to ensure that there are no instances of unauthorized access to the production program libraries.

The Chief, FMIS, has agreed to implement a compensating control to mitigate the risk associated with allowing access to production programs and has agreed to establish procedures for the Chief, Central Computer Operations Branch, to maintain a log of emergency program changes. The security coordinator within FMIS has agreed to use features of the security software to produce a report identifying access to the production libraries. This report will be reconciled to the log of emergency changes to ensure that no

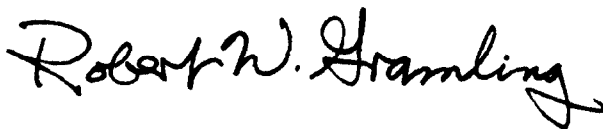
B-114839

unauthorized program changes have been made. The Commission's Chief Financial Officer told us that these changes were implemented in June 1992.

- - - - -

We would like to thank you and Commission personnel for the courtesy and cooperation extended to our audit team. Should you have any questions regarding these suggestions, please call Roger Stoltz or me at (202) 275-9406.

Sincerely yours,



Robert W. Gramling, Director
Corporate Financial Audits

(917661)