GAO

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

Accounting and Information
Management Division

B-114839

July 21, 1994

The Honorable Robert R. McMillan
Chairman, Board of Directors
Panama Canal Commission

Dear Mr. McMillan:

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, 1993 (GAO/AIMD-94-89, March 31, 1994).

In planning and performing our audit of the financial statements of the Commission, we identified certain matters regarding accounting procedures and internal control structure which could be improved. These include review and reconciliation of inventory records, recording of inventory receipts and issuances, general electronic data processing (EDP) controls over computer systems, and centralized responsibility over information assets.

Although these matters are not material in relation to the financial statements, they warrant the attention of management. The purpose of this letter is to advise you of these matters and to make suggestions for improvement. As appropriate, we discussed the matters addressed in this letter with Commission supervisory personnel and have included their comments for your information.

REVIEW AND RECONCILIATION OF PERPETUAL INVENTORY RECORDS' NEGATIVE INVENTORY BALANCES

Review of perpetual inventory records for unusual items and the resulting reconciliation and adjustment of records are important internal controls to ensure that inventory balances

are properly recorded and valued. The Commission counts inventory and reconciles the results with its inventory records throughout the year; however, it relies on its perpetual inventory records for reporting year-end balances. We found that the Inventory Management Branch does not review year end perpetual Storehouse Inventory Management System records for unusual or unreasonable balances. We found the fiscal year-end inventory records showed stock items with negative dollar values and negative quantities on hand. In addition, certain stock items showed negative dollar values with positive quantities on hand. Although reports are generated to identify negative inventory values and quantities on hand, there are no written procedures requiring the Inventory Management Branch to review and reconcile these reports. As a result, Inventory Management personnel did not investigate or correct negative inventory values or quantities at year-end. Although these negative values are not material to the year-end inventory balance, management can not be assured that inventory balances are reported accurately without proper reconciliation of perpetual inventory records.

We suggest that the Commission strengthen the controls and procedures in the inventory area by requiring Inventory Management Branch personnel to review the negative inventory reports and reconcile and correct negative inventory values and quantities on hand at year-end.

The Chief of the Systems Division stated that he will work with the Inventory Management Branch to develop and implement control procedures to ensure that year-end negative inventory balances are investigated and corrected.

RECORDING INVENTORY RECEIPTS AND ISSUANCES

We reported last year that the Inventory Management and Warehousing Branches were submitting daily batches of inventory data to the Computer Operations Division for keypunching without using turnaround transmittal documents to verify that all documents were received and processed. We also noted that the Computer Operations Division did not return the source documents to the Inventory Management Branch after processing. In addition, the Inventory Management and Warehousing Branches did not review daily reports of data entered to verify that all submitted data were correctly processed. Instead, daily batch and error reports were used solely to identify and research records

rejected by computer edit checks. Except for following up on edit rejects, management did not have procedures to ensure that all inventory data sent for processing were accurately received and processed.

During this year's audit, we found that management had not implemented control procedures to correct these weaknesses. However, at the completion of our audit, the Chief of the Systems Division and the Chiefs of the Inventory Management and Warehousing Branches advised us that they plan to implement procedures during fiscal year 1994 requiring that necessary inventory data reports and documents be generated and reviewed daily to ensure that all inventory data sent for processing are received and processed.

GENERAL EDP CONTROLS OVER COMPUTER SYSTEMS

We found weaknesses in some general EDP controls[1] over the Commission's computerized information systems. These weaknesses limit the effectiveness of the controls to ensure that financial data files and computer programs are protected from unauthorized access and modification. We believe that access control software can be more effectively implemented, and that passwords and user identifications (IDs) can be more effectively managed. In addition, controls to ensure the separation of duties can be strengthened.

Implementation of Access Control Software

The Commission uses an access control software package (ALERT) to provide system-level security over its computer resources. ALERT is installed on the computers used for the financial management system (FMS), E-mail, and marine traffic control but is not installed on the computer used for systems

---

[1]General EDP controls are the policies and procedures that apply to an entity's overall effectiveness and security of operations and that create the environment in which other related EDP controls operate. General controls include the organizational structure, operating procedures, software security features, and physical protections designed to ensure that only authorized changes are made to computer programs, that access to data is appropriately restricted, that back-up and recovery plans are adequate to ensure the continuity of essential operations, and that physical protection of facilities is provided.

development. Because the computers share online facilities and disk devices, it is possible for users of the systems development computer to gain unauthorized access to the FMS computer. We suggest that this exposure be decreased by installing ALERT on the computer used for systems development.

Further, the current implementation of ALERT software enables E-mail users to gain access to the Virtual Machine (VM) operating system, providing them with an unintended access path to financial data within FMS. We suggest that appropriate changes be made to remove this access path.

The Commission has also not implemented ALERT's capability to automatically log off users after a certain period of inactivity. This feature reduces the exposure caused by an unattended terminal. Since the Commission's management has been hesitant to implement this feature globally, we suggest selective implementation of this feature, tailored to each user department's operations, to improve controls over security access with minimal inconvenience to the user.

The Chief of Management Information Systems (MIS) stated that he agrees with the need for these improvements and has contracted with a security specialist to assist in expanding the implementation of the ALERT security software on the central computers. He further advised us that a detailed report and work program covering these areas and other security improvements was finalized in June and that implementation is now in progress as the first phase of a project expected to take several months.

Password and User ID Management

MIS generates and distributes a hardcopy list of new passwords to the user security coordinators to facilitate periodic password changes and to synchronize system-level passwords with application-level passwords. In addition, passwords were changed only at 6- to 12-month intervals. These practices increase the risk that passwords may be compromised and permit unauthorized system access.

We suggest that log-on IDs and passwords be changed more frequently, and that they no longer be printed. We also suggest that MIS explore the feasibility of using ALERT to automatically change passwords.

MIS does not currently have an effective procedure to ensure that inactive user IDs are removed from the system promptly. We noted during our review that approximately 25 percent of users had not used their log-on ID during the preceding 6 months. We suggest that MIS establish a new reporting procedure to (1) enable user security coordinators to periodically validate the access capabilities of their personnel and (2) update or remove IDs promptly.

The Chief of MIS stated that he agrees with these suggestions and is acting on these issues.

Controls Over Separation of Duties

Application maintenance programmers have incompatible duties in that they also maintain the internal application security database. The Chief of MIS believes that the organization is too small for a separate group to maintain the application security database. In addition, this database cannot provide an audit trail of modifications, nor are there facilities which would allow owners of applications to review and validate the database authorizations. We suggest that MIS modify the system to regularly provide application and dataset owners with reports of the authorizations in this database for their review. These controls will serve as a check over the activities of the application maintenance progammers. However, we also suggest that as the organization grows, maintenance programmers should be precluded from having access to the application security database.

The Chief of MIS stated that he agrees with our suggestions and is acting on these issues.

CENTRALIZED RESPONSIBILITY OVER INFORMATION ASSETS

We previously reported that 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 assets.[2] We suggested that this responsibility be assigned to an information

[2]Management Letter to Chairman, Board of Directors, Panama Canal Commission (GAO/AFMD-92-71ML, August 19, 1992).

security manager reporting to the Commission's senior management.

At the completion of our audit of the Commission's 1993 financial statements such a position still had not been established. However, the Commission requested, under an interagency agreement with the National Institute of Standards and Technology (NIST), that NIST perform a security review of the Commission to address this and other security concerns.

In its February 1994 report to the Commission, NIST recommended that the Commission appoint an Information Systems Security Program Manager. Regarding that report, senior managers said that it contains positive and useful recommendations that, for the most part, merit serious consideration by the Commission. The NIST report is currently under review by the Administrative Services Division and the Financial Management Information Systems Division.

We consider the Commission's request for outside assistance in evaluating its security environment an appropriate action. We believe that our suggestions, taken with those from the NIST report, provide a framework for positive organizational and procedural changes to enhance controls over access to computer resources.

We would like to thank the Commission for the courtesy and cooperation extended to our audit team. Should you have any questions regarding these suggestions, please call Linda Garrison at (404) 679-1902 or me at (202) 512-9406.

Sincerely yours,

Robert W. Gramling

Robert W. Gramling, Director
Corporate Financial Audits

(917690)