15-3797

15-3889

GAO

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

Accounting and Information
Management Division

B-260920

March 31, 1995

The Honorable Joe R. Reeder
Chairman, Board of Directors
Panama Canal Commission

Dear Mr. Reeder:

We have issued opinions on the financial statements of the Panama Canal Commission and its internal control structure and have reported on the Commission's compliance with applicable laws and regulations for the year ended September 30, 1994 (GAO/AIMD-95-98, March 31, 1995).

In planning and performing our audit of the Commission's financial statements, we identified certain matters regarding general controls[1] over the Commission's computer information systems which could be improved to strengthen the computer security environment. These include enhancing implementation of access control software, improving the organization and management of the management information systems (MIS) security, and formalizing MIS policies and procedures.

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. We

[1]General controls are policies and procedures that apply to an entity's overall effectiveness and security of computer operations and create the environment in which other related computer controls operate. General controls include the organizational structure, operating procedures, software security features, and physical protections designed to ensure that (1) only authorized changes are made to computer programs, (2) access to data is appropriately restricted, (3) back-up and recovery plans are adequate to ensure the continuity of essential operations, and (4) facilities are physically protected.

have discussed the matters addressed in this letter with Commission management and have included their comments as appropriate for your information.

COMPUTER INFORMATION SYSTEMS CONTROL ENVIRONMENT

In previous years, we reported[2] certain weaknesses in the Commission's computer information systems. These weaknesses increase the risk of unauthorized access and modifications to the Commission's computer programs and financial data. We also noted some weaknesses in the organization and management of MIS security that could limit the overall effectiveness of the MIS security environment.

In response to our reports, the Commission engaged the National Institute of Standards and Technology (NIST) and Legent (the firm that markets the Commission's security software) to review its computer security. Based on the report NIST issued in February 1994, the Commission's MIS management developed a Security Update Plan to address security issues.

We believe that this plan provides a framework for positive organizational and procedural changes to enhance controls over the Commission's computer resources. However, based on this year's audit, we suggest that the Commission review the Security Update Plan to ensure that the following issues are clearly addressed and that necessary changes are implemented as soon as possible.

IMPLEMENTATION OF ACCESS CONTROL SOFTWARE

The Commission uses access control software packages (ALERT/VM and ALERT/CICS[3]) to provide system-level security over its production computer resources. The current implementation of ALERT software, however, does not fully

---

[2]Management Letter to the Chairman, Board of Directors, Panama Canal Commission (GAO/AIMD-94-134ML, July 21, 1994; GAO/AFMD-93-23ML, September 10, 1993).

[3]ALERT/VM (Virtual Machine) software provides security at the VM operating-system level; ALERT/CICS (Customer Information Control System) provides security at the CICS on-line level.

and appropriately use available capabilities in the areas of (1) user passwords, (2) terminal access, and (3) protection of all data and programs.

User Passwords

Passwords are an important control to prevent unauthorized system access. To strengthen this control, passwords are changed periodically. Currently, the Commission's user passwords expire at 6-month intervals and its Virtual Machine (VM) initial passwords[4] do not expire. The 6-month interval between password changes increases the risk of compromised passwords and unauthorized access. We suggest that user passwords be changed every 60 to 90 days for general users and every 30 days for users having sensitive privileges, such as the security administrator, systems programmer, or branch chief. We also suggest that MIS management determine a reasonable expiration interval for VM initial passwords.

MIS management reported that password change policies are under review and the resulting changes are expected to be incorporated into the Security Update Plan and completed by June 1995.

Terminal Access

Although passwords help prevent system access by unauthorized users, they do not prevent unauthorized activity by authorized users. ALERT can be used to restrict users' access to specific times of the day and days of the week to control unsupervised activity, but the Commission is not using this capability. We suggest ALERT be used to restrict users' access to business hours or other appropriate time periods to help prevent unsupervised activity.

Another control technique to monitor system activity is automatically logging users off the computer system after a period of inactivity. This control reduces the exposure caused by an unattended logged-on terminal. We found that the Commission has not implemented ALERT's capability to automatically log off all users after a period of inactivity. We suggest implementing appropriate log-off intervals for all

[4]VM initial passwords are temporary passwords provided by MIS that are assigned to new users prior to their first system access. Upon initial access, the user is required to change this password to a personal password.

users. These log-off intervals can be tailored to each department's operations.

MIS management reported that pilot tests and detailed analyses are being conducted to determine appropriate log-off intervals. A decision on the final policies for the use of log-off intervals and for the restriction of users' access times is expected by June 1995.

Protection of All Data and Programs

ALERT access control software can be programmed to protect data and programs against unauthorized access by (1) programming specific access rules or definitions, which define the data a particular user can access, and (2) programming ALERT defaults that prevent access to data and programs when specific rules or definitions are missing. These ALERT defaults are an important compensating control to protect against programming oversights. However, we found that the Commission has not programmed the ALERT defaults to deny access when specific access rules or definitions are missing. As a result, certain data and programs may be unprotected. We suggest that the Commission program the ALERT security software to deny access to data and programs when other specific access rules are missing. According to MIS management, default protection is scheduled to be implemented by July 1995.

ORGANIZATION AND MANAGEMENT OF MIS SECURITY

In addition to improving the implementation of access control software, we found changes were needed in the organization and management of MIS security. We believe controls can be strengthened by ensuring the segregation of duties and assigning responsibility for MIS security to a full-time information systems security program manager.

Segregation of Duties

Segregation of duties within the MIS department is an important control to reduce the risk of unauthorized access to and modifications of computer programs and data. For example, separating the functions of application programming and computer operations provides an important control over unauthorized program changes or unauthorized changes to operations data.

Because the Commission's application programmers can run applications, they have access to financial and payroll data and programs. Some of these application programmers also have excessive on-line transaction privileges, giving them access to all financial and payroll data and programs. To reduce the risk of unauthorized changes, we suggest that production privileges granted to application programmers be appropriately restricted.

MIS management stated that these matters were corrected subsequent to our testing. We will follow up on this issue in next year's audit.

Centralized Responsibility for Information Assets

We have reported previously that responsibility for information security is fragmented throughout the Commission, with no branch or division having overall responsibility for data and physical security for the Commission's information assets. We suggested that this responsibility be assigned to an information systems security program manager. In its February 1994 report to the Commission, NIST made the same suggestion.

MIS management advised us that the Commission is actively planning to consolidate information security responsibilities and expects to staff this security program manager position by October 1995.

FORMALIZATION OF SECURITY POLICIES AND PROCEDURES

During this year's audit, we identified other weaknesses in MIS security policies and procedures which we believe to be attributable in part to the lack of centralized responsibility for information security. We found that the Commission had not adequately documented the MIS controls environment and personnel position descriptions and that personnel were not receiving adequate computer security training. We suggest that formal security policies and procedures--both Commission-wide and MIS-specific--be developed, documented, and implemented.

Documentation of the MIS Internal Controls Environment

Documentation of the software security architecture and internal control structure is particularly important to the Commission because security software is implemented by two MIS functions using different access control software. The lack of such documentation at the Commission has led to gaps and overlaps in software security. We suggest that the Commission develop detailed, technical documentation of its software security architecture and internal control structure.

According to MIS management, the Security Update Plan is scheduled to formalize security policies and procedures and document the software security architecture and the MIS internal controls environment. These two responsibilities will be the primary focus of the information systems security program manager.

Documentation of Personnel Position Descriptions

Having specific and up-to-date personnel position descriptions for all MIS personnel enables management to better define staff roles and responsibilities. However, we found that the position descriptions we reviewed for personnel with computer security responsibilities did not include security, making it difficult to hold individuals accountable for this area. We suggest that position descriptions for MIS personnel be updated to reflect all current security-related responsibilities.

According to MIS management, personnel position descriptions are being rewritten in accordance with new Office of Personnel Management standards and will reflect security-related duties as appropriate. This effort is expected to continue through 1996.

Computer Security Training

The Computer Security Act of 1987 requires MIS and other Commission personnel to receive computer security training at regular intervals. We found that this training was not occurring regularly and that the course being used to train Commission personnel in security awareness, policy, and procedures was not tailored to the Commission's operations. For instance, the course included security practices for

classified information, which the Commission does not process.

We suggest that MIS work with human resources development staff to develop an appropriate curriculum for computer security training and that all users and managers--including senior executives--be required to have such training at least annually.

According to MIS management, the security program manager, once appointed, will be responsible for coordinating with human resources development staff in developing the suggested security training program.

- - - - -

We would like to thank the Commission for the courtesy and cooperation extended to our audit team. We ask that the Commission keep us informed regarding corrective actions taken on these issues. Should you have any questions, please call Linda Garrison, Assistant Director, at (404) 679-1902 or me at (202) 512-9406.

Sincerely yours,

Robert W. Gramling

Robert W. Gramling, Director
Corporate Financial Audits

(917692)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Mail
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested