USAID

U.S. Agency for
International
Development

December 30, 1998

MEMORANDUM FOR DIRECTOR USAID/PERU, THOMAS GEIGER

FROM: for IG/A/ITSA, Theodore P. Alves Melinda Dempsey

SUBJECT: Audit of USAID/Peru's General Controls Over the Mission Accounting and Control System (MACS) (Audit Report No. A-527-99-001-P)

This report presents the results of our audit of USAID/Peru's General Controls Over MACS, which we performed in support of the Government Management Reform Act of 1994. Our audit found that USAID/Peru's general controls over MACS do not adequately protect against serious threats that include unauthorized access to MACS programs, data, and other computer resources. Unauthorized access can result in improper disclosure, modification, or loss of data and assets. To illustrate, sensitive financial information such as account identification numbers, bank identification numbers, and bank routing numbers, are vulnerable to unauthorized access, change, and disclosure. USAID/Peru's operations are also vulnerable to disruption of service in the event of computer failures. The critical general control that USAID/Peru did not implement was development of an effective computer security program.

This deficiency is part of broader deficiencies that affect USAID overall. In September 1997, the Office of Inspector General (OIG) reported that USAID had not implemented an effective computer security program. The Assistant Administrator for Management (AA/M) agreed to implement an effective program, and USAID has begun to do so. Although the agency-wide computer security program hinders USAID/Peru's efforts to ensure adequate security, USAID/Peru is ultimately responsible for ensuring that its resources and people are protected. Therefore, this report addresses issues that are the responsibility of USAID/Peru and contains one recommendation that can be implemented by USAID/Peru. Because USAID is in the process of developing an agency-wide computer security program in response to prior OIG recommendations, we have not repeated earlier recommendations to develop such a program agency-wide.

A companion report "Audit of Access and System Security Controls over USAID's Mission Accounting and Control System (MACS)" addresses access and system software control deficiencies identified during this audit that are the responsibility of the Telecommunications and Computer Operations Division within the Bureau for Management's Information Resources Management Office (M/IRM/TCO).

We discussed these issues with your Executive Officer and Systems Manager and provided them the detailed worksheets describing specific control weaknesses.

In the December 11, 1998 response to our draft report, the Mission Director concurred with the recommendation and is taking corrective actions to strengthen the general controls over MACS. We have attached, as Appendix II, the complete response to our draft report.

Thank you for the cooperation and assistance extended to our staff during this audit.

Background

General controls are the policies, procedures, and management structure that help to protect an organization's computer systems and operations. Primary objectives of general controls include safeguarding data and assets, protecting computer application programs and system software from unauthorized modification, and ensuring continued operations in case of unexpected interruptions.

To assist in developing and sustaining general controls, GAO prepared the Federal Information System Controls Audit Manual (FISCAM), Volume I- Financial Statement Audits. GAO divided the controls into six critical elements. The elements include: (1) a security program, (2) access controls, (3) application software development and change controls, (4) segregation of duties, (5) system software, and (6) service continuity. Appendix III describes each element. We used FISCAM to conduct our audit of the general controls over MACS.

MACS is a computer-based accounting and financial management system that provides information to mission management as well as to USAID/Washington. MACS defines the guidelines, procedures, and standards used to record, analyze, and report accounting data. To illustrate, MACS contains computer programs that perform accounting and financial management functions such as reconciling accounting records for specific periods, archiving historical data, maintaining security, and recovering from system failures. The system also contains data files and special programs to assist system operations. MACS is an on-line, interactive processing system that employees use to continuously update and post transaction data using computer workstations. MACS is written in COBOL and is designed to operate at USAID missions using the UNIX operating system on a Sun Microsystems computer.

The Information Resources Management Division (USAID/Peru IRM) under the Executive Office is responsible for operating MACS. USAID/Peru IRM is responsible for: (1) establishing information system computer processing requirements and implementing an effective security program; (2) processing all requests for computer access to the system; and

(3) providing system computer services. The Controller's Office is the primary user of MACS. It relies on MACS to carry out its responsibilities and to support the Mission's accounting, budgeting, cash management, financial analysis, and financial reporting operations.

Audit Objective

The audit was designed to answer the following objective:

- **Are USAID/Peru's general controls over the Mission Accounting and Control System effective?**

Our audit focused on the general controls that affect USAID/Peru's ability to safeguard assets and maintain MACS' sensitive financial data. We examined the controls in place to determine whether they were designed and implemented properly. Specifically, we assessed four of GAO's six control elements: the security program, access controls, segregation of duties, and system software controls. We did not evaluate the application software development and change controls because the Mission did not develop application software. Also, because other Missions can provide some continuity of service, we limited the assessment of service continuity.

A full description of our scope and methodology is contained in Appendix I.

Summary of Results

USAID/Peru's general controls over MACS are not effective. As a result, sensitive data, assets, and computer resources are vulnerable to unauthorized access, modification, loss, or destruction. USAID/Peru's efforts to maintain adequate general controls are significantly hindered by agency-wide computer security deficiencies, including a lack of guidance and standards about maintaining a computer security program. In spite of the lack of guidance, however, USAID/Peru is ultimately responsible for ensuring the security of its computer facilities and data. Because the primary deficiency that is under USAID/Peru's control is the lack of an effective security program[1], this report focuses on USAID/Peru's security program.

[1] Because deficiencies in access and system software controls at USAID/Peru are primarily controlled by USAID Washington, we issued a separate report describing those deficiencies (Audit of the Access and System Software Security Controls Over the Mission Accounting and Control System, Report No. A-527-99-002-P, December 31, 1998).

USAID/Peru Needs to Implement an Effective Security Program

USAID/Peru has not implemented an effective security program for MACS. Although the Executive Officer and Systems Manager did implement several components of a security program, including (1) assigning user identifications and passwords, (2) requiring backup copies of MACS data to be stored off-site, and (3) using encrypted password files and suppressed passwords, the program did not meet the requirements of the Computer Security Act of 1987, Office of Management and Budget's (OMB) Circular A-130[2], or USAID's Automated Directive Systems (ADS)[3].

An organization-wide computer security program provides the foundation on which effective computer security practices can be implemented. By establishing a framework for planning and managing activities to assess risks, develop and implement security procedures, and monitor the effectiveness of the procedures, the security program helps assure that sensitive data and resources will be protected in a cost-effective manner. Without a security program, risks may not be clearly understood, controls may not be effective, and large amounts might be spent to protect against low-risk threats.

The major requirements and practices that USAID/Peru has not fully implemented are:

- conducting risk assessments of computer operations;
- maintaining current security plans for sensitive systems;
- preparing and testing an adequate contingency plan; and
- monitoring and evaluating the effectiveness of its security program.

USAID/Peru IRM managers agreed to strengthen the security program and advised us of actions they had taken, or planned to take, to address these deficiencies. In particular, a committee comprised of the Controller, Executive Officer, Deputy Executive Officer, Security Specialist, and the System Manager will be formed to determine how the mission will take action to address its security program.

[2] According to the Computer Security Act of 1987, Federal agencies with computer systems that process sensitive information are required to identify and develop security plans for these systems and to provide security training to persons managing, using, and operating these systems. The Office of Management and Budget's (OMB) Circular A-130 establishes a minimum set of controls to be included in Federal automated information systems security programs. These controls include assigning security responsibilities, preparing security plans, conducting security reviews, accrediting systems, and providing security incident reporting capabilities.

[3] The ADS, Chapter 551, Automated Information Systems Security, documents the agency's security policies and procedures for information systems security and lists the specific headquarters and mission responsibilities.

USAID/Peru Needs to Adequately Assess Risks

Risk assessments are critical components of the security program because they identify assets of the system, threats that could affect the confidentiality, integrity, or availability of the system, system vulnerabilities to threats, and potential impacts from threat activity. An assessment also identifies the protection requirements to control the risk and selection of cost-effective security measures. Failure to conduct risk assessments increases the chance that (1) existing threats have not been identified, the impacts from threats have not been considered, and (2) protection requirements have not been analyzed.

USAID/Peru provided us a documented risk assessment. However, it has not conducted a comprehensive assessment of MACS in order to identify the unique risks that exist for MACS. Additionally, it has not related the MACS data and programs to any risk-based analysis of threats and vulnerabilities, and it has not adequately discussed the planned efforts to implement recommendations identified as a result of the analysis.

USAID/Peru Needs to Develop a Security Plan

As required by the Computer Security Act and OMB Circular A-130, USAID/Peru must prepare and implement security plans to protect systems containing sensitive data. The security plans document the security requirements of systems and describe how the agency will meet the requirements. USAID/Peru did not have a current security plan for MACS or the hardware system that supports MACS.

Our September 1997 report on USAID's compliance with federal computer security requirements[4] noted that the agency did not require the preparation of security plans. However, IRM/Washington, in a draft information systems security program plan, stated that it will take actions to comply with OMB's requirements to develop and implement security plans for sensitive systems. This draft plan further stated that each system manager will develop and update security plans for their organization.

USAID/Peru Needs an Adequate Contingency Plan

Disruption of computer operations could adversely affect USAID/Peru's ability to achieve its mission. To ensure that critical operations can continue in emergencies, USAID's policy requires a plan to cope with potential loss of operational capability.

[4] Audit of USAID's Compliance with Federal Computer Security Requirements, Audit Report No. A-000-97-008-P, September 30, 1997.

Although USAID/Peru has prepared a contingency plan, the plan is not adequate. For example, the plan did not specifically provide for the recovery of its critical systems and when MACS was unavailable for eight days in May 1998, there was no formal plan to obtain emergency or back-up support from another mission. Without an adequate contingency plan and a test of that plan, USAID/Peru faces unnecessarily high risks that its mission will be seriously impaired should a major service disruption or disaster occur.

USAID/Peru Needs to Evaluate and Monitor Its Security Program

USAID/Peru has not adequately evaluated or monitored its computer security requirements. That is, the Mission did not systematically monitor the security program, but relied on the system administrator to initialize, set, and maintain the computer security program. The Executive Officer, who has responsibility for security, has not developed procedures to determine if the controls were operating as intended or evaluated the effectiveness of the program in communicating policies, raising awareness levels, and reducing incidents. For instance, USAID/Peru has not examined the system for vulnerabilities that can result from improper use of controls or mismanagement. Subsequently, vulnerabilities such as the easily guessed passwords and improperly protected system files existed and controls were not effective in preventing control weaknesses that exposed MACS data to unauthorized use, modification, and destruction.

Conclusion

Effective general controls require attention to maintain the integrity, availability, and performance of sensitive systems in a complex computer environment. While USAID/Peru has taken some measures, its general controls were ineffective in key control areas. If USAID/Peru is to adequately protect sensitive data and systems from unauthorized access, disclosure, and loss, it must implement an effective computer security program. The ineffective general controls are part of broader deficiencies that affect USAID overall. In September 1997, the OIG reported that USAID had not implemented an effective computer security program. The Assistant Administrator for Management (AA/M) agreed to implement an effective program, and USAID has begun to do so. Although the agency-wide computer security program hinders USAID/Peru's efforts to ensure adequate security, USAID/Peru is ultimately responsible for ensuring that its resources and people are protected.

Recommendations

We recommend that the Director, USAID/Peru direct the Executive Officer to strengthen USAID/Peru's general controls by:

Recommendation No. 1: **Developing a computer security program that includes:**

1.1 conducting risk assessments of computer operations;

1.2 maintaining current security plans for sensitive systems;

1.3 preparing and testing an adequate contingency plan; and

1.4 monitoring and evaluating the effectiveness of its security program.

Management Comments and Our Evaluation

In response to the draft audit report, the Mission Director for USAID/Peru concurred with the recommendation contained in the report. The Mission Director stated that USAID/Peru is taking the following actions to further strengthen the general controls:

- establishing a Computer Security and Development Team chaired by the Mission's Deputy Director;
- issuing mission orders to establish and reinforce security policy and procedures for handling sensitive but unclassified information, describing user responsibilities, and improving access procedures; and
- scheduling IRM/Washington to conduct a risk assessment of USAID/Peru's computer operations.

USAID/Peru's comments are reproduced in Appendix II.

Based on the above, a final management decision has been reached on the recommendation. USAID's Office of Management Planning and Innovation (M/MPI) should be advised when final action is complete.

SCOPE AND METHODOLOGY

Scope

Our audit of USAID/Peru's general controls over MACS was limited to identifying and testing computer operations controls that were applied to all computer applications on the Sun Microsystems Server. Such controls included the Mission's security program, access controls, segregation of duties, and system software controls. As part of the security program evaluation, we did not assess the security-related personnel screening policies and procedures. Our audit also did not include an assessment of the application software development and change controls because the mission did not develop application software. Because other missions operating in similar computer environments can offer emergency support, we limited our assessment of the service continuity control area and combined it with the security program control.

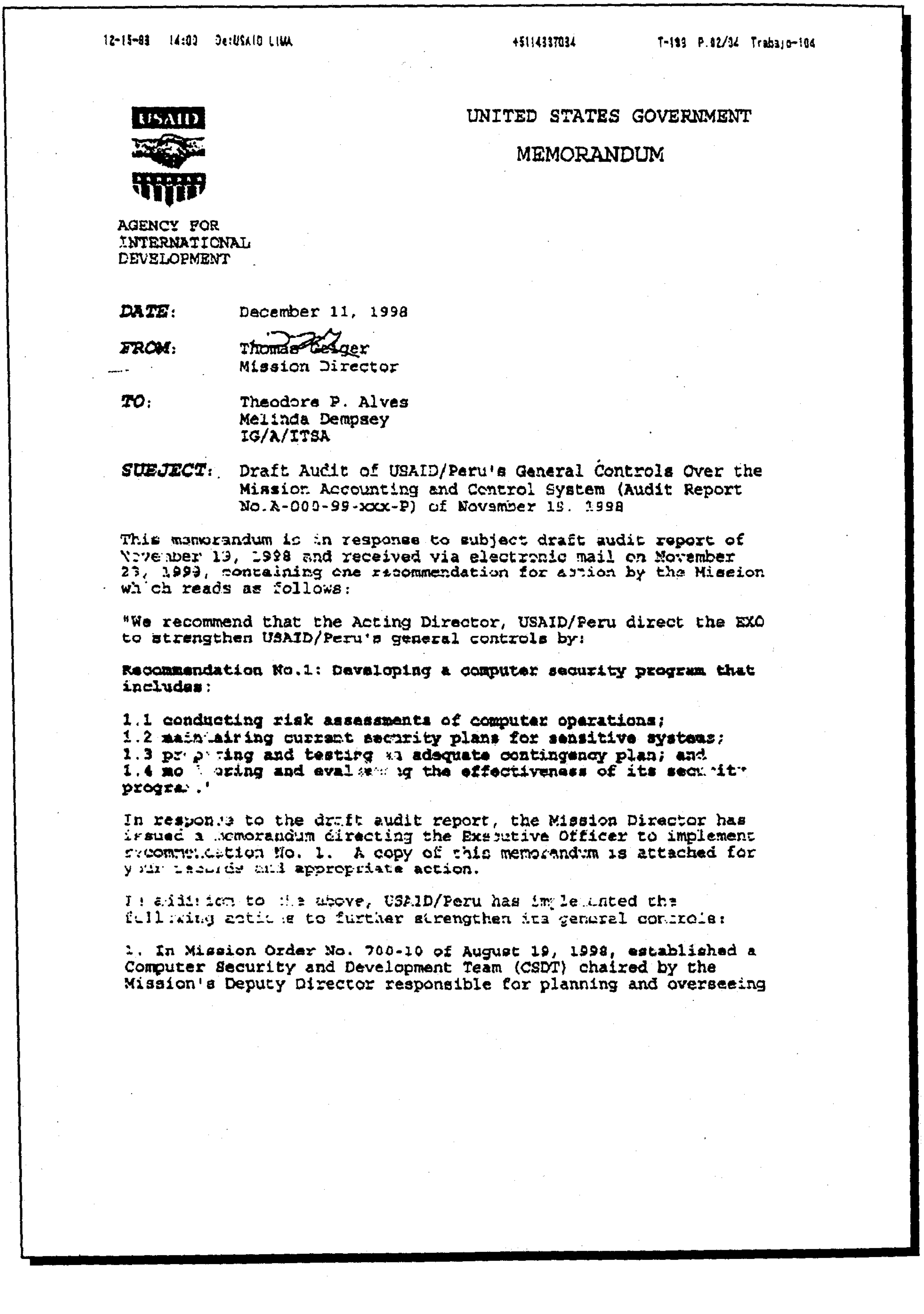
We audited to determine if USAID/Peru has: (1) ensured adequate computer security administration; (2) protected its MACS data and programs from unauthorized access; (3) provided segregation of duties involving the responsibilities for computer operations and security; and (4) prevented unauthorized changes to systems software. To the extent that general control deficiencies existed, we identified the factors that caused the deficiencies. We also identified management actions that would help reduce the adverse impacts and correct the deficiencies.

We conducted the audit in accordance with generally accepted government auditing standards. The audit was conducted at USAID/Peru between June 15, 1998, and July 2, 1998.

Methodology

We used GAO's Federal Information System Controls Audit Manual to evaluate USAID/Peru's general controls over MACS. We identified and reviewed the information system's general control policies and procedures. We documented the extent to which USAID/Peru implemented the controls. Through discussions with the Executive and Controller Offices, including the systems manager, we noted what controls existed. We tested and observed the operation of controls to determine if they were designed and operating effectively. Our tests included assessing the computer system supporting MACS to determine whether we could gain access to MACS' sensitive data.

We reviewed an evaluation of the Embassy at Lima, Peru, dated August 1997, performed by the Department of States' Security and Intelligence Oversight. The purpose of the report was to assess strengths and weaknesses of the Embassy post, office or function. Results of the work conducted indicated weaknesses in USAID's implementation of security procedures. We reviewed recent reports under provision of the 1982 Federal Managers' Financial Integrity Act. We also reviewed USAID's Automated Directive System, Chapter 551 on Automated Information Systems Security, the Computer Security Act of 1987, and the OMB Circular A-130.



12-15-98 14:03 De:USAID LIMA +5114337034 T-193 P.02/34 Trabajo-104

USAID

AGENCY FOR
INTERNATIONAL
DEVELOPMENT

UNITED STATES GOVERNMENT

MEMORANDUM

DATE: December 11, 1998

FROM: Thomas Geiger
Mission Director

TO: Theodore P. Alves
Melinda Dempsey
IG/A/ITSA

SUBJECT: Draft Audit of USAID/Peru's General Controls Over the Mission Accounting and Control System (Audit Report No.A-000-99-xxx-P) of November 19, 1998

This memorandum is in response to subject draft audit report of November 19, 1998 and received via electronic mail on November 23, 1998, containing one recommendation for action by the Mission which reads as follows:

"We recommend that the Acting Director, USAID/Peru direct the EXO to strengthen USAID/Peru's general controls by:

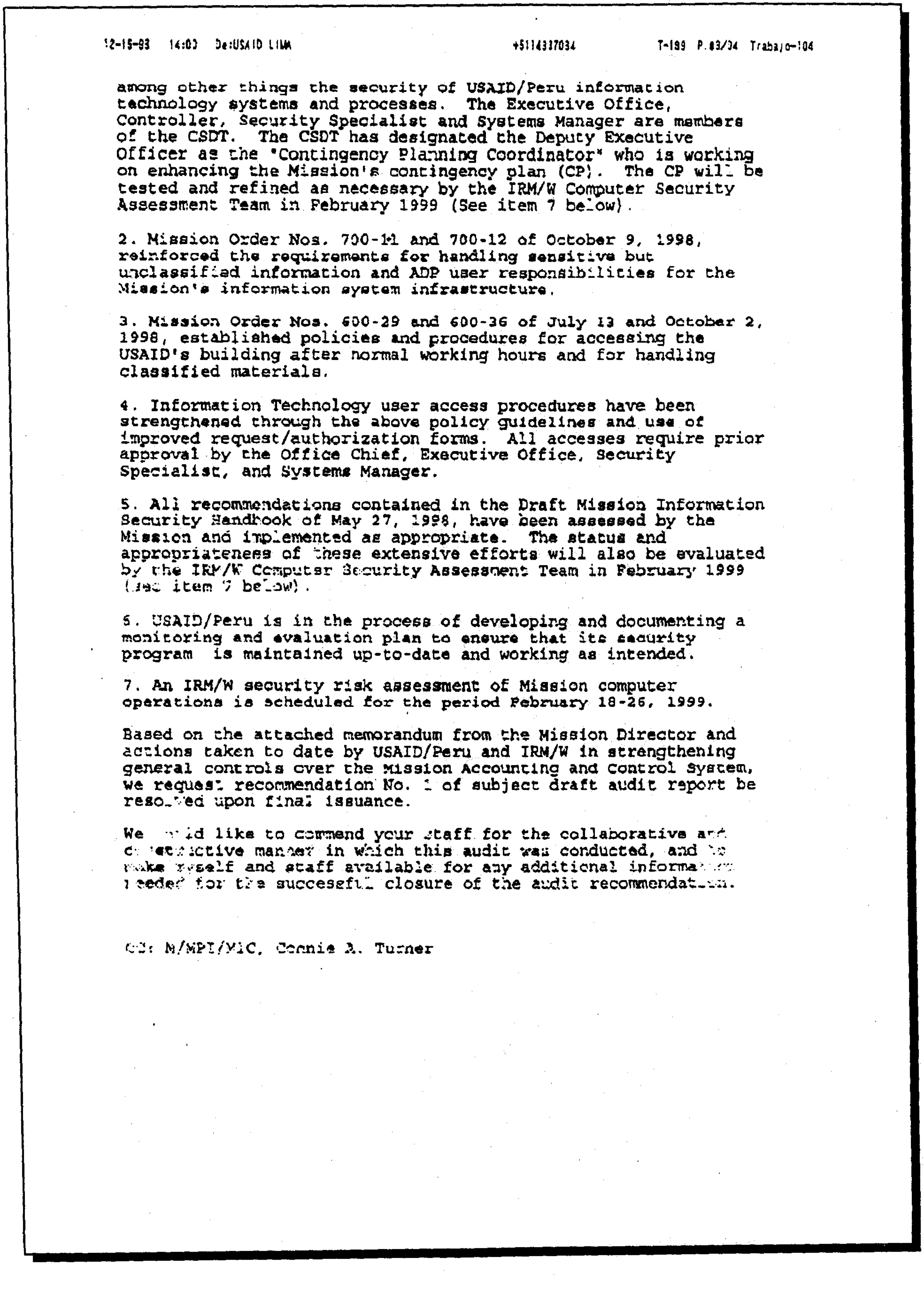
Recommendation No.1: Developing a computer security program that includes:

1.1 conducting risk assessments of computer operations;
1.2 maintaining current security plans for sensitive systems;
1.3 preparing and testing an adequate contingency plan; and
1.4 monitoring and evaluating the effectiveness of its security program."

In response to the draft audit report, the Mission Director has issued a memorandum directing the Executive Officer to implement Recommendation No. 1. A copy of this memorandum is attached for your records and appropriate action.

In addition to the above, USAID/Peru has implemented the following actions to further strengthen its general controls:

1. In Mission Order No. 700-10 of August 19, 1998, established a Computer Security and Development Team (CSDT) chaired by the Mission's Deputy Director responsible for planning and overseeing



among other things the security of USAID/Peru information technology systems and processes. The Executive Office, Controller, Security Specialist and Systems Manager are members of the CSDT. The CSDT has designated the Deputy Executive Officer as the "Contingency Planning Coordinator" who is working on enhancing the Mission's contingency plan (CP). The CP will be tested and refined as necessary by the IRM/W Computer Security Assessment Team in February 1999 (See item 7 below).

2. Mission Order Nos. 700-11 and 700-12 of October 9, 1998, reinforced the requirements for handling sensitive but unclassified information and ADP user responsibilities for the Mission's information system infrastructure.

3. Mission Order Nos. 600-29 and 600-36 of July 13 and October 2, 1998, established policies and procedures for accessing the USAID's building after normal working hours and for handling classified materials.

4. Information Technology user access procedures have been strengthened through the above policy guidelines and use of improved request/authorization forms. All accesses require prior approval by the Office Chief, Executive Office, Security Specialist, and Systems Manager.

5. All recommendations contained in the Draft Mission Information Security Handbook of May 27, 1998, have been assessed by the Mission and implemented as appropriate. The status and appropriateness of these extensive efforts will also be evaluated by the IRM/W Computer Security Assessment Team in February 1999 (see item 7 below).

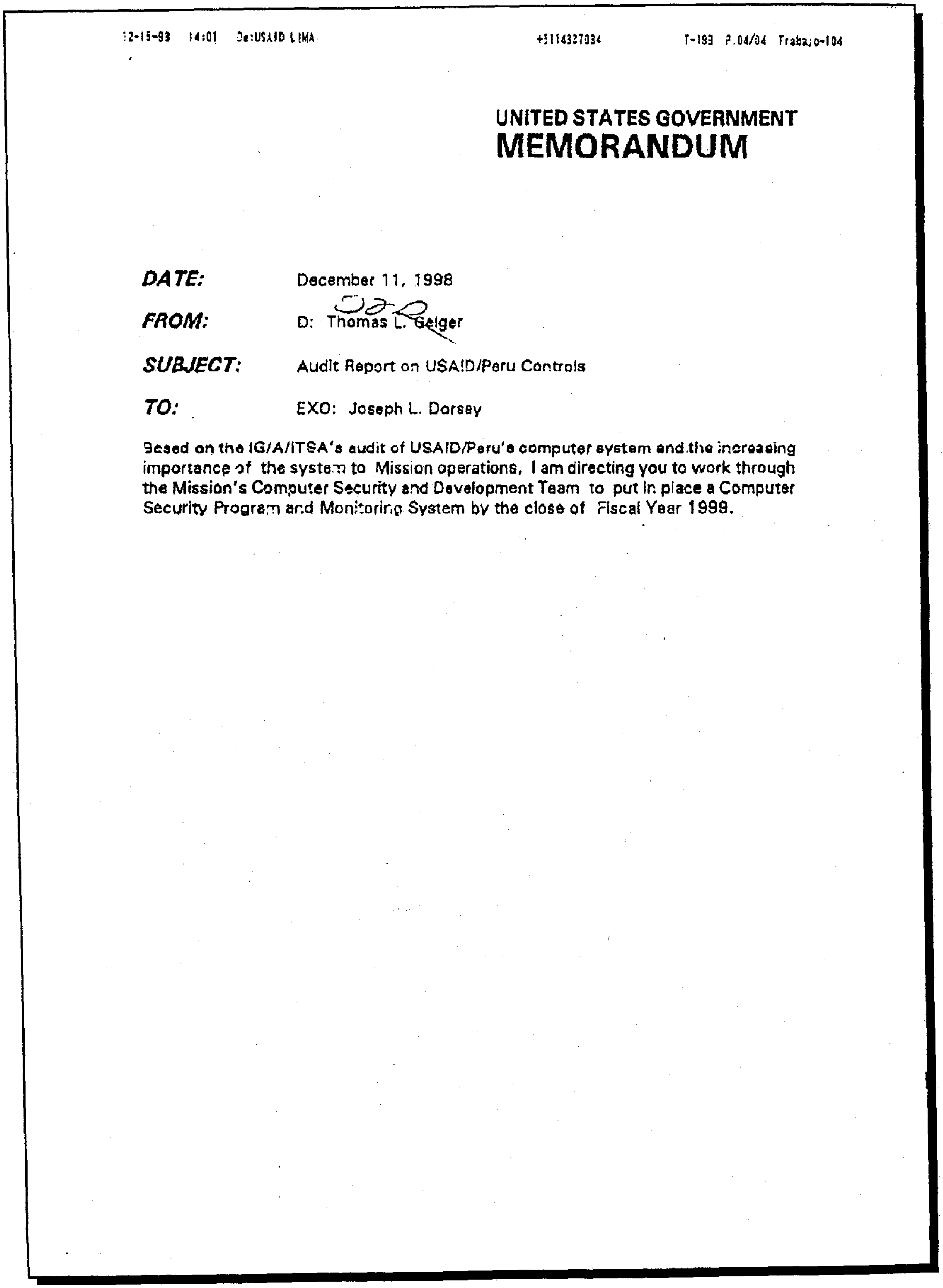
6. USAID/Peru is in the process of developing and documenting a monitoring and evaluation plan to ensure that its security program is maintained up-to-date and working as intended.

7. An IRM/W security risk assessment of Mission computer operations is scheduled for the period February 18-26, 1999.

Based on the attached memorandum from the Mission Director and actions taken to date by USAID/Peru and IRM/W in strengthening general controls over the Mission Accounting and Control System, we request recommendation No. 1 of subject draft audit report be resolved upon final issuance.

We would like to commend your staff for the collaborative and constructive manner in which this audit was conducted, and to make myself and staff available for any additional information needed for the successful closure of the audit recommendation.

CC: M/MPI/MIC, Connie A. Turner



12-15-98 14:01 De:USAID LIMA +5114327034 T-193 P.04/04 Trabajo-104

UNITED STATES GOVERNMENT
MEMORANDUM

DATE: December 11, 1998

FROM: D: Thomas L. Geiger

SUBJECT: Audit Report on USAID/Peru Controls

TO: EXO: Joseph L. Dorsey

Based on the IG/A/ITSA's audit of USAID/Peru's computer system and the increasing importance of the system to Mission operations, I am directing you to work through the Mission's Computer Security and Development Team to put in place a Computer Security Program and Monitoring System by the close of Fiscal Year 1999.

GAO'S CATEGORIZATION OF GENERAL CONTROLS

No.	Critical Elements	Description
1.	Security Program	Provides the framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.
2.	Access Controls	Limits or detects access to computer resources. Thus, these controls protect the resources from unauthorized modification, loss, and disclosure.
3.	Application Software Development and Change Controls	Prevents unauthorized programs or modifications to an existing program from being implemented.
4.	Segregation of Duties	Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations.
5.	System Software	Limits and monitors access to the power programs and sensitive files that (1) control the computer hardware, and (2) secure applications supported by the system.
6.	Service Continuity	Ensures that, when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.