



U.S. Agency for
INTERNATIONAL
DEVELOPMENT

Washington, D.C.

September 25, 2001

MEMORANDUM FOR A-CIO, Peter Benedict

FROM: IG/A/ITSA, Melinda G. Dempsey

SUBJECT: Audit of USAID's Compliance with the Provisions of the
Government Information Security Reform
(Report No. A-000-01-002-P)

This memorandum is our report on the subject audit. Thank you for the level of importance you attach to information security. Your comments on the draft report are included in Appendix II.

This report contains ten recommendations for your action. Based on your comments, management decisions have been reached on these recommendations. Please notify the Office of Management Planning and Innovation (M/MPI) when final actions on these recommendations are completed, and request closure.

I appreciate the cooperation and courtesy extended to my staff during the audit.

Table of Contents	Summary of Results	3
	Background	4
	Audit Objective	5
	Audit Findings	5
	USAID’s Management of its Information Systems Security Program Needs to be Improved	6
	USAID’s Policies and Procedures Need to be Improved	10
	Additional Comments Regarding USAID’s Information Systems Security Program	13
	Management Comments and Our Evaluation	15
	Appendix I - Scope and Methodology	16
	Appendix II - Management Comments	18
	Appendix III – Implementation of Security Requirements in USAID’s Mission Critical Systems	22

Summary of Results

The government information security reform (GISR) provisions included in the fiscal year 2001 Defense Authorization Act, requires Inspectors General to perform annual evaluations of agencies' security programs. [page 4] The objective of this audit was to determine if USAID had implemented an effective information systems security program that meets the provisions of GISR. [page 5]

The results of the audit showed that while USAID recognized the need to develop and initiate an agency-wide information systems security program, such a program had not been fully implemented across the agency. [page 5] This audit identified policy and procedures that could be clarified and enforced to help ensure more effective security program management. [pages 10-13] The underlying cause for USAID's security program weaknesses is the lack of a strong centralized function to oversee, enforce, and coordinate security and related functions. [page 12]

In a concurrent audit, the OIG also identified serious general controls¹ weaknesses that place financial systems at significant risk of unauthorized disclosure and modification of sensitive data, misuse or damage of resources, or disruption of critical operations. [page 9] The weaknesses may also hamper USAID's ability to produce reliable financial information. A major contributing factor for ineffective general controls is the security program deficiencies.²

To correct the identified weaknesses in the information systems security program, we are making recommendations to the Chief Information Officer (CIO) to ensure that sufficient resources and top management attention are committed to implementing an effective information systems security program—one that includes (1) centralizing security functions; (2) improving the current policies and procedures; (3) implementing monitoring systems to ensure compliance with policy and procedures; (4) improving the incident response capability; (5) providing sufficient training; and (6) requiring corrective actions for identified vulnerabilities. The OIG also included a recommendation to the CIO to ensure that a clear management structure and responsibilities and accountability are implemented throughout the agency. [pages 9, 10, 12 and 13]

¹ General controls are the structure, policies, and procedures that affect the overall effectiveness and security of computer operations. These include security management, system security software, and controls designed to ensure that access to data and programs is restricted, computer duties are segregated, only authorized changes are made to computer programs, and plans are adequate to ensure continuity of operations.

² We are currently drafting the report on USAID's general controls, which will have restricted distribution.

Because the agency's security program deficiencies apply to both this and the concurrent audit on USAID's general controls over financial systems, implementing the recommendations described in the general controls report will also address a number of the deficiencies in this report. The general control report's recommendations are not repeated in this report. This report provides a high-level summary of the agency-wide security program weaknesses and the companion report will address the general controls in detail, including the agency-wide security program.

Background

On October 30, 2000, the President signed into law the fiscal year 2001 Defense Authorization Act (P.L. 106-398) including the provisions on government information security reform. The provisions seek to improve program management and evaluations of agencies' security efforts for unclassified and national security systems.

Major requirements of GISR include:

- Annual agencies reviews.
- Annual Inspector General or independent evaluations.
- Annual Office of Budget and Management's reports to Congress that summarizes the Inspectors General and Agencies' reports.
- Annual agency performance plan that describes time periods for implementing the agency-wide security program.
- Agencies incorporating security practices throughout life cycle of all systems.

GISR also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) incident security capability is established, (3) security is integrated into the capital planning and investment process, and (4) critical assets are protected within the enterprise architecture. GISR further re-enforces the need for agencies to develop and implement agency-wide security programs for its assets and operations by requiring agencies to follow the Office of Budget and Management's policy to: (1) assess risks and determine needs, (2) implement appropriate policies and related controls, (3) promote awareness of security risks, and (4) monitor and evaluate policy and control effectiveness.

In September 1997, the Office of Inspector General reported that USAID had not implemented a security program that met the requirements of the

Computer Security Act of 1987 or the Office of Management and Budget's Circular A-130. USAID then identified its overall computer security program as a material weakness in its fiscal year 1997 Federal Managers' Financial Integrity Act and fiscal years 1998 through 2000 Accountability Reports. USAID plans to correct this material weakness in September 2003.

Since 1997, USAID has undertaken efforts to develop a program and to improve its ability to protect its computer systems. For example, USAID has (1) appointed an Information Systems Security Officer, (2) developed a draft Information Systems Security Program Plan, (3) identified mission critical systems, (4) conducted risk assessments at some overseas missions led by the information systems security team, (5) updated policy on information systems to implement government information security reform legislation, (6) issued guidance to the missions on the assignment of information security roles, (7) adopted a process to approve systems for processing, and (8) established an Information Systems Security Working Group and Information Security Advisory Group.

Audit Objective

The FY 2001 Defense Authorization Act (P.L. 106-398) including the provisions on the government information security reform mandated this audit. As a result, the objective of this audit was to answer the following question:

Has USAID implemented an effective information systems security program that meets the provisions of government information security reform (GISR)?

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

Audit Findings

Has USAID implemented an effective information systems security program that meets the provisions of government information security reform (GISR)?

USAID has not fully implemented an effective³ information systems security program that meets the provisions of GISR. Although USAID has made significant progress in developing an information systems security program, it has not implemented a program that allows USAID officials to comprehensively manage the risks associated with USAID's operations and systems. Specifically, USAID had not: (1) enforced its policies and procedures to ensure that they were implemented

³Effective is defined as designing controls that are properly implemented and working as intended.

appropriately and (2) provided adequate guidance to incorporate security into some of its information technology processes. Such deficiencies exposed USAID to unacceptable risks that resources will not be adequately protected. The deficiencies occurred because USAID had not implemented a centralized function that has oversight and ensures that USAID meets security requirements.

USAID's Management of its Information Systems Security Program Needs to be Improved

GISR requires agency officials to ensure that they effectively implement and maintain information security policies and procedures. Even though USAID has developed policies and procedures to protect its systems and operations, it had not followed or adhered to them. Specifically, USAID had not, as required: assessed risks for all of its mission critical systems, provided mandatory security training to employees, generally monitored policy compliance or the effectiveness of the controls agency-wide, and fully implemented security incidents reporting. In addition, the OIG found that contingency plans were not completed and that deficiencies and vulnerabilities identified by USAID's security reviews were not being corrected.

Our testing of USAID information systems security included both, Washington, D.C. headquarters operations as well as eight overseas missions as listed in Appendix I. At headquarters and the eight USAID missions the OIG determined that:

- GISR requires agencies to develop and implement information systems security programs that establish a security control structure and framework that include conducting periodic risk assessment. USAID has developed a risk assessment process that integrates security awareness training and corrects system vulnerabilities encountered by the information systems security team immediately. USAID has also conducted scans of headquarter systems and completed risk assessments for 12 of 81 missions. However, at headquarters and six of the eight USAID missions we visited, risk assessments were not done on major systems. USAID plans to conduct more assessments and has begun to conduct assessments of the major field accounting system.

Furthermore, USAID has identified eight systems as mission critical and assigned security responsibilities for all eight. However, Appendix III illustrates that the eight mission critical

systems did not meet some major requirements (e.g., security plans were not prepared for all systems, etc.). USAID's information systems, some of which are operated and maintained by other federal government agencies and Riggs Bank, are critical to its mission.

- GISR requires agencies to provide security awareness training. USAID provided employees and contractors in headquarters with security awareness training as part of the new employee's orientation program. But, USAID still needs to provide specific training to key personnel to carry out their security responsibilities such as conducting a risk assessment and preparing security plans. In addition, annual refresher briefings have not been provided to all employees. For its overseas missions, USAID had no structured security-training programs, as required, at seven of the eight missions that the OIG visited. USAID has begun to implement a training program utilizing compact disk and web-based instructions with an automated tracking system. Without training, USAID's staff was not adequately trained to perform their security responsibilities and systems are unprotected.
- GISR calls upon agencies to perform periodic testing and evaluations of the information systems security program. As previously stated, some scans were conducted for both headquarters and mission systems. While USAID headquarters did conduct scans of all the missions, periodic testing and evaluations of the security program were not performed at any of the eight USAID missions. Such testing and evaluation ensures that controls are functioning effectively and identified deficiencies are corrected. Without centralized monitoring, USAID has no assurance that its security policies are implemented consistently across the agency.
- GISR require agencies to implement incident response capability. Incident response and reporting capabilities were not fully implemented at headquarters and at seven of the eight USAID missions. USAID has published policy guidance that instructs USAID personnel on how to report a security incident. However, this incident response reporting has not been fully implemented. For example, it does not yet provide timely reports of the identified incidents. The Information Systems Security Officer stated that they are working to improve the process, as well as developing a database to capture the information. A pilot Cyber Defense Center has been established in headquarters and intrusion sensors added in Cairo, Egypt to provide alerts and reports on significant events affecting systems security. At the time of the OIG's work, USAID

had not approved or fully funded the one center in headquarters. The lack of incident response reporting hinders USAID's ability to track agency-wide trends and assess the threats so that changes to controls can be made as needed.

- Lastly, the Office of Management and Budget's Circular A-130 requires agencies to develop contingency plans. However, USAID has not implemented comprehensive plans to ensure continuity of systems and disaster recovery operations. A continuity of operations plan (COOP) has been documented, but it is outdated. The COOP provides the capability to continue operations during a crisis that renders an organization's headquarters unusable. Although we were told that USAID was not ready for an April 2002 Interagency Test Exercise to test agencies readiness capabilities, USAID is (1) in the process of hiring expertise in emergency preparedness, and (2) working on its electronic vital records, which will be included in the Automated Directives System. In addition, well-documented plans for disaster recovery and continuity of operations had not been developed to ensure USAID could continue to fulfill its mission while responding to natural disasters, accidents, or other major and minor interruptions. The audit identified plans that had not been completed. For example, five of the eight missions provided no contingency plans for their systems.

The OIG also noted that although USAID identified deficiencies through its own security reviews, the results were not used to ensure security compliance. As a result, the security reviews conducted by USAID have provided limited benefits for USAID's security program. For example,

- USAID has developed strong configuration management policies that generate reports of deficiencies. However, there is no evidence that any actions are taken to correct deficiencies noted during the reviews that are performed as part of the process. As a result, deficiencies remain uncorrected and systems are vulnerable.
- USAID's security staff conducted a broad range of vulnerability scanning operations, and reported the findings to the appropriate individuals involved and to USAID network managers. These reports identified some of the same vulnerabilities that were noted during this audit, indicating that no action was taken. USAID's information systems security team and the network management staff also designed a checklist to identify and eliminate a number of serious technical vulnerabilities that are routinely noted in

systems. The audit revealed that the checklist was not applied at the time we visited the overseas missions and for some headquarters systems. Again, systems remain vulnerable.

The problems identified above are caused by the lack of a strong mechanism to ensure that security activities are periodically monitored, tested and evaluated; and that appropriate corrective actions were taken. It is unclear who is providing oversight to review compliance with policies and procedures. For example, although the Information Systems Security Officer (ISSO) is responsible for overseeing and executing the operational information systems security activities, he cannot direct the offices to correct deficiencies, such as the ones identified during the audit. Moreover, the ISSO reports to the Office of Information Resources Management instead of the CIO. As a result the ISSO's authority and responsibility for enforcing security policies is limited because of his organizational placement.

Moreover, USAID's guidance on information systems security states that the Deputy Assistant Administrator, Bureau for Management serves as the Chief Information Officer. The CIO is responsible for directing, managing, and providing policy guidance and oversight with respect to all USAID information resource management activities. However, since the CIO does not directly report to the Administrator, the CIO is not in the best position to provide the necessary leadership, oversight, and enforcement for information security.

As a result of the security program's deficiencies, USAID's systems are highly vulnerable to external and internal unauthorized intrusions, use, disclosure, modifications, loss, and/or impairment. Examples of common problems are: poorly chosen passwords, inadequate access controls, and inadequate segregation of duties. Until USAID fully implements an information systems security program, its critical assets will remain at risk to attacks and threats.

Recommendations regarding the CIO and ISSO's authority and responsibilities will be made in the report on USAID's general controls.

Recommendation No. 1: We recommend that the Chief Information Officer obtain evidence that security requirements have been applied to USAID's mission critical systems. For those systems that are operated by other agencies and organizations, the responsible Assistant Administrator, the Chief Financial Officer, the Director of Human Resources, or the Director of the Office of Procurement shall provide the Chief Information Officer evidence that proper protection exists for those systems.

Recommendation No. 2: We recommend that Chief Information Officer provide and document that USAID employees in key security positions obtain training that allows them to conduct their security responsibilities.

Recommendation No. 3: We recommend that the Chief Information Officer conduct a study to determine the feasibility of monitoring controls, intrusion detection, and additional sensors for sensitive systems.

Recommendation No. 4: We recommend that the Chief Information Officer develop and implement a management oversight process by assigning responsibility and accountability for correcting identified information security vulnerabilities to designated individuals. The process should include a reporting mechanism that regularly tracks the status of all vulnerabilities, including actions taken to correct them.

USAID's Policies and Procedures Need to be Improved

GISR requires federal agencies to develop and implement information security policies, procedures, and controls sufficient to protect systems. These policies and procedures should be examined in relation to other information management laws and guidance, such as the Clinger-Cohen Act of 1996 and the Office of Management and Budget's Circular A-130.

USAID has responded to the requirement to develop information security policies, procedures and controls. For example, USAID had developed its security policies for information systems in the Automated Directives Systems (ADS)⁴ Chapter 545 "Information Systems Security". The most recent revisions of the policy were made in June 2001 to incorporate GISR. USAID's policies mandated specific actions, and defined and assigned security responsibilities, ranging from the Administrator to end-users within USAID. USAID has also developed checklists with recommended safeguards to apply to its systems to reduce threats and vulnerabilities.

However, some of USAID's policies and procedures do not adequately incorporate security into information technology processes as required by GISR. Such examples include USAID's capital planning and investment process, enterprise architecture process, and contractor-

⁴ USAID's Automated Directives System (ADS) is the agency's official, written guidance to its employees on policies, operating procedures, and delegations of authority for conducting Agency business.

provided services. In addition, some important USAID security documents are draft and not yet approved.

- USAID has developed a plan for processing capital planning and investment management control. This plan is USAID's basis for identifying, prioritizing and managing its portfolio of capital assets compatible with the enterprise infrastructure to achieve performance and compliance goals. However, the plan does not adequately address the integration of security into the overall capital planning and investment management control process or provide clear guidance to program managers on how to report security requirements. Security costs were included in USAID's Exhibit 53 submitted to Office of Management and Budget, however, the audit found that the security program and security requirements are not adequately reported in all USAID's fiscal year 2002 Capital Asset Plans and Justifications. Without clearly integrating security into all processes, security requirements may not be implemented in a cost-effective manner.

USAID's Administrator also approved the establishment of an Information Technology Council in June 2001 to provide investment control for information systems. One of its goals is to monitor information technology modernization efforts. The Council will convene at least quarterly to make executive decisions on policies, procedures, investment priorities, and funding related to the full range of matters covered by the Clinger-Cohen Act of 1996. This Council should help to ensure that security is incorporated into the investment process.

- USAID developed a Target Enterprise Information Architecture System Design Report to identify systems that support USAID's business areas. A review of the report indicated that: (1) a number of the security safeguards were undefined in each of the architecture's layers and (2) no policy guidance or standard security products existed for implementing the undefined safeguards. As a result, systems may be added to USAID's environment without proper security controls and safeguards.
- USAID has not documented its methodology for evaluating if contractor-provided services have met security requirements. While security requirements are addressed in the contracts for the Principal Resource for Information Management Enterprise-wide contractor, it is not known if all agency contracts have security language. In practice, the OIG noted that, for USAID's mission critical systems that are operated by other agencies and Riggs Bank, USAID requested reports to identify the current status of the systems' security.

However, USAID has not yet received the reports. Without this methodology in place, USAID cannot be assured that its data processed by other agencies and contractors is protected.

Finally, four of USAID's important guidelines for its security program are drafts. For example, the draft of USAID's Information Systems Security Program Plan (ISSPP) is dated January 26, 2001 and as of July 18, 2001, was still in draft and not approved. The ISSPP is the framework for USAID's overall security program. It describes the needs for implementing security and proposes the budget that will be necessary to implement the program. Other important documents that also remain in draft include those that provide guidance on the risk assessment and incident reporting processes⁵.

The above deficiencies existed because USAID's security program lacks a strong centralized security function to ensure that policies and procedures adequately address the key components of security management. Currently, USAID's responsibility for information system security is decentralized and fragmented. Divided between the Chief Information Officer, the Office of Information Resources Management, the Office of Administrative Services, the Office of Security, and the overseas missions makes the coordination and implementation of security extremely difficult if not impossible because no one office has overall responsibility.

The shortcomings in the policies and procedures can lead to inconsistent or inappropriate actions to protect data and systems. Without adequate policies and procedures, management does not have the assurance that controls are working, and established policies and procedures are being followed.

Recommendation No. 5: We recommend that the Chief Information Officer centralize security functions to oversee, enforce, and coordinate security and related functions.

Recommendation No. 6: We recommend that the Chief Information Officer coordinate the revision of appropriate Automated Directives System Chapters and any other supporting guidance to include and/or clarify the government information security reform-mandated requirements, especially those that pertain to incorporating security into the investment process, enterprise architecture, and contractor-provided services.

⁵ The draft documents are: (1) USAID Information Systems Security Program Plan (ISSPP), dated 1/26/01; (2) USAID Risk Assessment Manual, dated 7/21/98; (3) USAID Security Incident Handling Response Policy and Procedures, dated 10/31/00; and (4) USAID Incident Response Capability (IRC) Handbook Coordinating Draft dated 7/13/01.

Recommendation No. 7: We recommend that the Chief Information Officer provide instructions to program managers to include security requirements in the information technology investment process and report them on Capital Asset Plans.

Recommendation No. 8: We recommend that the Chief Information Officer finalize and approve the following four draft documents: (1) USAID Information Systems Security Program Plan; (2) USAID Risk Assessment Manual; (3) USAID Security Incident Handling Response Policy and Procedures; and (4) USAID Incident Response Capability Handbook Coordinating Draft.

Additional Comments Regarding USAID's Information Systems Security Program

The GISR provisions also addressed Presidential Decision Directive 63, performance measures to assess risk and other security issues, and the system's life-cycle process. The OIG reviewed USAID's policies and procedures for the above topics and had the following comments.

- GISR addresses the integration of information and information technology security program with its critical infrastructures protection responsibilities. The Presidential Decision Directive 63 (PDD 63) tasked Federal Agencies to develop critical infrastructure protection plans. The OIG audit found that USAID had not developed such a plan. USAID's position is that the Department of State has responsibility for completing the plan because of its designation as lead agency for foreign affairs. USAID's Information Systems Security Officer stated that USAID was not tasked under PDD 63 to prepare the plan. The OIG is recommending that USAID address its plans to protect critical infrastructures. The OIG believes that if USAID implements an effective information systems security program within USAID, it also will succeed in protecting systems, which are a part of the nation's critical infrastructures. However, this and other OIG reports and USAID's reviews, have showed that USAID is not adequately protecting its systems or infrastructures.
- USAID has not established specific performance measures for its security program—a prerequisite for effective feedback and reporting on the program's goals. As a result, standards are not in place to programmatically measure the performance of security controls and

hold program managers accountable. In addition, USAID did not provide documentation on the measures of performance to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system.

- USAID has a draft Information Systems Security Program Plan that documents the framework for its information systems security program. The plan and other security policy documents required agency personnel to incorporate security into the life cycle of the information systems. The OIG has not audited a system through an entire life cycle in the last two years. However, the OIG noted during the implementation of Phoenix—USAID's financial accounting system—a security review was conducted prior to system's implementation. Because of major system changes, a second review is scheduled for October. The OIG is not making a recommendation to address this issue.

Recommendation No. 9: We recommend that the Chief Information Officer document the agency's decision on the critical infrastructures protection plan.

Recommendation No. 10: We recommend that the Chief Information Officer develop specific performance measures that include timetables and approaches to address deficiencies in its information security program.

**Management
Comments and
Our Evaluation**

In response to our draft report, the acting Chief Information Officer agreed with the recommendations in the report and is planning to implement the recommendations. Consequently, management decisions have been reached on the ten recommendations.

USAID management stated that it formally adopted an Information Systems Security Program Plan (ISSPP) on August 17, 1999, but the updated version of the 1999 final ISSPP is currently in draft form. USAID contractors provided the 1999 ISSPP to the OIG. However, the 1999 ISSPP is marked as a “preliminary coordination draft”, even though the cover states it was approved for implementation. The January 2001 ISSPP mentioned in the audit report is a draft update to the 1999 ISSPP.

Management’s complete responses are included in Appendix II.

**Scope and
Methodology**

Scope

The Office of Inspector General in Washington conducted an audit in accordance with generally accepted government auditing standards to determine if USAID had implemented an information systems security program that meet the provisions of the Government information security reform. The audit was conducted from June 18, 2001 to September 12, 2001.

The OIG assessed USAID's information systems security program, including the agency's compliance with GISR and the Office of Management and Budget's guidelines, and USAID's effectiveness in implementing policies and procedures for information systems security. During the audit, the OIG reviewed security policies and procedures, and the overall organizational and administrative security framework for developing and implementing the agency program.

The OIG audit focused on a subset of the financial systems at both headquarters and the overseas missions. The audit coverage was limited to the following financial systems: (1) Phoenix—USAID's financial accounting and management system that operates in Washington, D.C.; (2) the field-based accounting systems; and (3) systems operated and maintained by other agencies: Department of Agriculture's National Finance Center for personnel/payroll; Riggs National Bank for loans processing; and Department of Health and Human Services for letter of credit processing. The audit also included reviewing USAID's time and attendance and network systems.

The OIG did not analyze the adequacy of security controls that are in place or controls over classified or national security systems. According to agency officials, USAID is an end-user of national security systems and the owners of these systems include the Department of State and the Central Intelligence Agency.

Methodology

To evaluate USAID's security program for information systems, the OIG not only reviewed official documentation but held discussions with USAID officials responsible for the information systems security program, including the Chief Information Officer, the Information Systems Security Officer (ISSO), and contractors that were working on USAID security projects. Additionally, USAID's practices were compared with (1) GISR, (2) the General Accounting Office's Federal

Information System Controls Audit Manual (FISCAM), (3) the Office of Management and Budget's (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, and (4) the Clinger-Cohen Act of 1996.

Concurrent with this audit, the OIG has also reviewed general controls at USAID headquarters in Washington, D.C. and eight overseas missions (Cairo, Egypt; Accra, Ghana; Budapest, Hungary; Nairobi, Kenya; Bamako, Mali; Managua, Nicaragua; Lagos/Abuja, Nigeria; and Kiev, Ukraine). In the general controls audit, the OIG reviewed mission-specific information technology security policies, guidance, and information. This information included risk assessment documents, security plans, and contingency plans. The OIG also determined whether USAID's policies and practices were in compliance with FISCAM. Contractors were obtained to perform internal penetration testing at missions (yet to be completed) and headquarters. The results of the general controls audit were used to support our conclusions for this audit.

Additionally, the OIG obtained specific information from the Information Systems Security Officer and staff regarding security of USAID's mission critical systems, as well as observed the agency's assessment process for meeting the GISR provisions. Lastly, the OIG obtained status reports on the recommendations from the previous computer security audit report.

Management Comments

MEMORANDUM

TO: IG/A/ITSA, Melinda G. Dempsey

FROM: Acting Chief Information Officer, Peter Benedict

SUBJECT: Draft Report on the Audit of USAID's Compliance with the Provisions of the Government Information Security Reform (Report No. A-000-01-xxx-P)

Thank you for the opportunity to respond to the subject draft report. USAID recognizes that we have weaknesses in information systems security, and we are initiating improvements to mitigate many of the issues identified in your report. Your report on General Controls is going to be critical to this effort as well, and we look forward to seeing it. We are currently working to complete our reporting requirements to the Office of Management and Budget (OMB) as tasked by Topic 14 of the Government Information Security Reform (GISR), OMB Memo 01-24. This effort will require that we provide a high level plan of action and milestones matrix for the program and each mission critical system to correct security weaknesses identified through annual program reviews, independent evaluations, and other reviews or audits. We will also develop a more detailed implementation plan. The implementation plan will include areas in which USAID needs to improve such as: (1) security program management; (2) access controls; (3) software development and change controls; (4) segregation of duties; (5) operating system(s) software controls; and (6) service continuity. Specific comments regarding the draft report and recommendations are noted below.

Status of Information Systems Security Program Plan

At the top of page 5 and throughout the draft report, you reference the "draft Information Systems Security Program Plan". It is more accurate to convey that the USAID CIO formally adopted an Information Systems Security Program Plan (ISSPP) on August 17, 1999. An updated version of the 1999 final ISSPP is currently in draft form.

Draft Report Recommendations

Recommendation No. 1: We recommend that the Chief Information Officer obtain evidence that security requirements have been applied to USAID's mission critical systems. For those systems that are operated by other agencies and organizations, the responsible Assistant Administrator, the Chief Financial Officer, the Director of Human Resources, or

the Director of the Office of Procurement shall provide the Chief Information Officer evidence that proper protection exists for those systems.

Management Decision: We agree with this recommendation. By September 2002, USAID intends to have security plans in place for USAID-operated systems. We will also confirm that systems operated by other agencies have plans that include and adequately meet USAID security requirements.

Recommendation 2: We recommend that the Chief Information Officer provide and document that USAID employees in key security positions obtain training that allows them to conduct their security responsibilities.

Management Decision: We agree with this recommendation but believe that it is feasible only if supervisors make employees available for training. While some information systems security training materials have already been made available, and some designated employees in key security positions trained, many still need training. Funding has been requested to meet this requirement. We anticipate that this will be done by the end of FY2003.

Recommendation 3: We recommend that the Chief Information Officer conduct a study to determine the feasibility of monitoring controls, intrusion detection, and additional sensors for sensitive systems.

Management Decision: We agree with this recommendation. USAID systems owners will first need to assess the sensitivity of USAID information stored, processed or transmitted on USAID systems. The degree of sensitivity of specific data is an essential factor in determining appropriate security controls, and identifying an appropriate level of risk for managers to accept as part of Agency operations. Once the relative level of sensitivity is established, determining appropriate, cost-effective technical controls will be possible. In addition to technical controls, management oversight and review will be essential to ensure compliance with information security policies and procedures. USAID is completing the development of a pilot Cyber Defense Center and expects that an evaluation of the concept will be complete by the end of FY2002. Funding has been requested for the Cyber Defense Center and needed intrusion detection sensors. If this funding is provided, the Cyber Defense Center will be functional by the end of FY2002.

Recommendation 4: We recommend that the Chief Information Officer develop and implement a management oversight process by assigning responsibility and accountability for correcting identified information security vulnerabilities to designated individuals. The process should include a reporting mechanism that regularly tracks the status of all vulnerabilities, including actions taken to correct them.

Management Decision: We agree with this recommendation. Part of our responsibility under GISR to OMB will be to develop a remediation plan, which will include individuals responsible for taking appropriate action. As indicated in the first part of this memo, USAID will be preparing quarterly reports to OMB on the status of our plan. USAID's Information Systems

Security Officer (ISSO) will be responsible for assessing the adequacy of security activities by systems owners. We will formally recommend an accountability mechanism and a delegation of authority for the ISSO to mandate security reviews by systems owners to the Administrator by the end of calendar year 2001. The CIO plans to have a management tracking mechanism in place by February 2002.

Recommendation 5: We recommend that the Chief Information Officer centralize security functions to oversee, enforce, and coordinate security and related functions.

Management Decision: We agree with this recommendation. We will address it in the course of USAID's ongoing reorganization. As a first step, ISSOs have been designated in writing for all mission critical systems. By March 2002, the CIO will provide an Action Memorandum to the Administrator regarding the implications for the Agency-wide reorganization. This issue will also be included for discussion on the next Information Security Advisory Group (ISAG) agenda.

Recommendation 6: We recommend that the Chief Information Officer coordinate the revision of appropriate Automatic Directives System Chapters and any other supporting guidance to include and/or clarify the government information security reform-mandated requirements, especially those that pertain to incorporating security into the investment process, enterprise architecture, and contractor provided services.

Management Decision: We agree with this recommendation. We will also address this issue in the course of USAID's ongoing reorganization. By February 2002, the CIO will work with M/OP to develop standardized security contract clauses to be included in all USAID information technology (IT) related contracts. By March 2002, the CIO will provide an Action Memorandum to the Administrator regarding the implications for the Agency-wide reorganization. This issue will also be included for discussion on the next Information Security Advisory Group (ISAG) agenda. By the end of FY2002, the CIO will review relevant ADS chapters, identify those needing modifications to strengthen security, and submit recommended changes to the responsible ADS authors.

Recommendation 7: We recommend that the Chief Information Officer provide instructions to program managers to include security requirements in the information technology investment process and report them on Capital Asset Plans.

Management Decision: We agree with this recommendation. By March 2002, the CIO will modify the Capital Investment Handbook to include a detailed process for developing, documenting, and budgeting for security requirements.

Recommendation 8: We recommend that the Chief Information Officer finalize and approve the following four draft documents: (1) USAID Information Systems Security Program Plan; (2) USAID Risk Assessment Manual; (3) USAID Security Incident Handling Response Policy and Procedures; and (4) USAID Incident Response Capability Handbook Coordinating Draft.

Management Decision: We agree with this recommendation. As indicated above, a final version of the 1999 ISSPP is already available. The CIO will review and finalize all current draft versions of documents by June 2002. However, newer drafts will continue to be created to reflect constantly developing Federal guidance, and to keep our documents current.

Recommendation 9: We recommend that the Chief Information Officer document the agency's decision on the critical infrastructures protection plan.

Management Decision: We agree with this recommendation. The CIO will document this decision by February 2002.

Recommendation 10: We recommend that the Chief Information Officer develop specific performance measures that include timetables and approaches to address deficiencies in its information security program.

Management Decision: We agree with this recommendation. Our remediation plan will include specific performance measures, timetables and approaches. We will report our progress to OMB quarterly. The initial plan will be submitted to OMB by October 31, 2001.

<i>IMPLEMENTATION OF SECURITY REQUIREMENTS IN USAID'S MISSION CRITICAL SYSTEMS</i>								
	MISSION CRITICAL SYSTEMS							
SECURITY REQUIREMENT	AETA	DHHS	GSS	MACS	NFC	NMS	PHX	RLMS
Security Plan Prepared	NO	NO ⁶	YES	NO	YES ⁷	YES	YES	NO ⁸
Certification/Accreditation Performed	NO	NO	NO	NO ⁹	NO	YES	YES	NO
Risk Assessment Conducted	NO	NO	NO ¹⁰	NO	YES	NO	NO	NO
Contingency Plan Prepared	NO	NO	NO	NO	NO	NO	NO ¹¹	NO
System Responsibility for Security Assigned	YES	YES	YES	YES	YES	YES	YES	YES

Mission Critical Systems:

- AETA - American Electronic Time and Attendance
- DHHS - Letter of Credit System
- GSS - General Support System – USAIDNET
- MACS - Mission Accounting and Control System
- NFC - National Finance Center
- NMS - New Management System
- PHX - Phoenix
- RLMS - Riggs Loan Management System

⁶ USAID has cross-serviced its letter of credit processing of grantee advances and liquidations to the Department of Health and Human Services (DHHS) payment management system.

⁷ USAID has cross-serviced its personnel and payroll processes for US direct hire employees to NFC. NFC's security plan and security risk assessment are dated 9/28/00 and address the virtual private network interface.

⁸ USAID has outsourced standard Credit Reform transactions to Riggs National Bank.

⁹ USAID has started the C&A process and conducted risk assessments for MACS in overseas missions.

¹⁰ USAID officials stated that risk assessments have been conducted for the GSS; however, these risk assessments were not provided to the OIG during the audit.

¹¹ While Phoenix does have a contingency plan, the plan does not include all the elements as required by appropriate guidance.