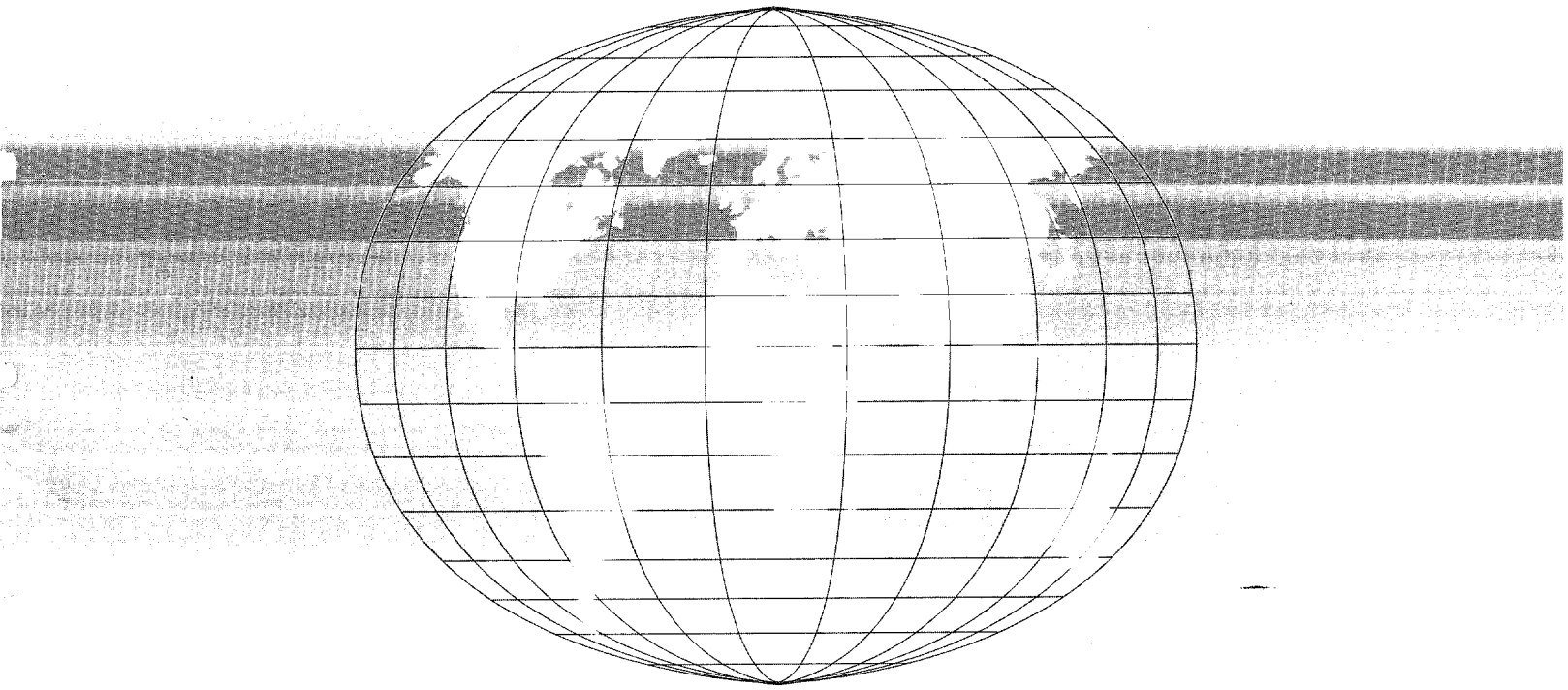
PD-ABP-626

Report of Audit

Audit of USAID's Compliance With Federal Computer Security Requirements

Audit Report No. A-000-97-008-P
September 30, 1997



IG/A/ITSA

OFFICE OF INSPECTOR GENERAL
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

U.S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

Office of
Inspector General

September 30, 1997

MEMORANDUM FOR M/B/OD, Richard C. Nygard

FROM: AIG/A, Everette B. Orr

SUBJECT: Audit of USAID's Compliance with Federal Computer Security Requirements (Audit Report No. A-000-97-008-P)

This report shows that USAID did not implement an effective security program that met the requirements of the Computer Security Act of 1987 or the OMB Circular A-130. The fundamental security requirements and practices that USAID did not implement were assigning security responsibilities, requiring and implementing security plans for all sensitive systems, and assessing all sensitive systems to ensure that they are protected. These deficiencies exposed USAID to unacceptable risks that resources will not be adequately protected from fraud or misuse, and that sensitive data and systems will not be adequately protected from loss or destruction. These deficiencies occurred because USAID did not implement an adequate system of management controls to support an effective computer security program. This report contains three recommendations (see page 19).

In the September 26, 1997 response to our draft report, the Acting Assistant Administrator for Management concurred with the recommendations. The response provided suggestions and additional information to clarify the meaning of several statements in the draft report. Based on our review of the response, we revised the report where appropriate. We have attached, as Appendix II, the complete response to the draft report.

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

Background

The increasing complexity of technology and the proliferation of computers have resulted in a greater commitment of USAID's resources to computer operations and a wide range of computer applications. USAID makes extensive use of information technology in serving the public and managing resources while executing its programs. However, this increased dependence on computers has caused a corresponding increased vulnerability to fraud, waste, and abuse. Agencies, including USAID, are thus increasingly exposed to the risk of unauthorized modification of data; destruction of computer resources; disruption of operations; and compromise or loss of resources, including sensitive agency information. Federal legislation, Office of Management and Budget (OMB) directives, and General Accounting Office (GAO) reports on information technology security highlight the need to develop and maintain adequate security over computerized information.

Among the significant laws and guidelines requiring agencies to maintain an effective computer security program are the Computer Security Act of 1987 (Public Law 100-235) and OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems."

The Computer Security Act of 1987

The purpose of the Computer Security Act of 1987 (Public Law 100-235) is to improve the security of sensitive information maintained in Federal computer systems by establishing minimum acceptable security practices. The Act requires Federal agencies to protect information by: (1) identifying sensitive systems, (2) developing and implementing security plans for sensitive systems, and (3) establishing a training program to increase security awareness and knowledge of accepted security practices. The Act further defines sensitive information as "any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs..." For example, financial and privacy information is considered sensitive.

OMB Circular No. A-130, Appendix III—Security of Federal Automated Information Systems

Appendix III of OMB Circular A-130, which implements the requirements of the Computer Security Act, directs agencies to establish a security program and maintain an adequate level of security for sensitive systems and information.

Specifically, the circular requires agencies to[1]:

(1) assign responsibility for security,

(2) develop system security plans,

(3) screen users,

(4) establish security training programs,

(5) develop incident reporting capabilities,

(6) assess risk,

(7) plan for contingencies, including disasters,

(8) review security safeguards, and

(9) obtain authorization before processing data.

USAID's Major Systems

According to records maintained by the Office of Information Resources Management (IRM), USAID maintains 61 application systems that process information to support its operations. USAID has identified five of the sixty-one systems as major application systems that process sensitive data in USAID/Washington:

- American Electronic Time and Attendance System (AETA) is used by timekeepers to maintain employees' biweekly time and attendance records.
- Financial Accounting and Control System (FACS) is USAID's financial management system for USAID/Washington activities.
- New American Payroll Systems (NAPS) performs personnel and payroll functions.

---

[1] The process applies to both application and support systems. Application systems are combinations of hardware and software that support a specific mission related function. Examples are systems for payroll, personnel, or accounting). General support systems consist of hardware and software to provide general data processing and telecommunication support for a number of applications (examples are data processing centers, local area networks, or wide area networks).

- Revised Automated Manpower and Personnel System (RAMPS) performs resource management functions such as tracking employee assignments and evaluations, providing staffing patterns, and monitoring training.

- New Management System (NMS) is USAID's newly deployed integrated system to perform accounting, acquisition and assistance, budgeting, and operations functions.

In addition to these major application systems, IRM maintains general support systems, including one that provides telecommunications and network connectivity among various applications and users.

Automated Information Systems' Security Responsibilities

Several organizations are responsible for the security of computer resources, as shown in Appendix III. The Administrator has delegated the primary responsibility for ensuring the security of automated information to the Office of Information Resources Management (IRM). Within IRM, the Information Policy and Administration Division (IPA) formulates policies and procedures, establishes and implements security awareness training, conducts security reviews, assists with contingency plans, and evaluates security technologies. The Telecommunications and Computer Operations Division is responsible for ensuring that the facilities which include general support systems are capable of operating in compliance with security policies and procedures. The Systems Development and Maintenance Division is responsible for ensuring that the application systems operate in compliance with security policies and procedures.

Establishing and executing the Continuity of Operation Program Plan is the responsibility of the Office of Administrative Services. System and program managers are responsible for implementing security guidelines at their locations. In overseas missions, the Executive Officer and system managers are responsible for operational security.

Audit Objective

This audit was conducted as a first step to address the overall security issues at USAID. Because of the concerns expressed by the Inspector General, Congress, and the General Accounting Office regarding the security of federal information systems, we conducted this audit to gain an understanding of USAID's policies and procedures for protecting its sensitive systems and the data they maintain.

The objective of this audit was to answer the following question.

> Did USAID implement a security program incorporating policies and procedures that meet the requirements of the Computer Security Act of 1987 and the OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"?

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

Audit Findings

USAID did not implement an effective security program that met the requirements of the Computer Security Act of 1987 or the OMB Circular A-130. The fundamental security requirements and practices that USAID did not implement were: assigning security responsibilities, requiring and implementing security plans for all sensitive systems, and assessing all sensitive systems to ensure that they are protected. Such deficiencies exposed USAID to unacceptable risks that resources will not be adequately protected from fraud or misuse. These deficiencies occurred because USAID did not implement an adequate system of management controls to support an effective computer security program.

USAID Did Not Meet Federal Security Program Requirements

USAID's policies and procedures governing automated systems security are contained in USAID's Automated Directive System (ADS) Chapter 551, "Automated Information Systems Security" and Handbook 6, "Security". Our comparison of USAID policies and procedures to the OMB security requirements showed that USAID had incorporated policies and procedures to address eight of the nine security requirements identified by OMB. However, the missing requirement, that agencies prepare a security plan, is significant because the security plan provides the foundation for an effective computer security program. Our analysis of the extent to which USAID procedures were effective in implementing OMB requirements found that USAID had not effectively implemented seven of the nine OMB security requirements.

Table 1 shows the extent to which USAID complies with the OMB security requirements.

Table 1

USAID'S COMPLIANCE WITH THE REQUIREMENTS OF OMB CIRCULAR A-130

OMB Circular A-130 Requirements	Do USAID's policies address A-130 requirements?		Has USAID adequately implemented the A-130 requirements?	
	Yes	No	Yes	No
(1) Assign responsibility for security	X			X
(2) Develop and implement security plans for application and general support systems		X		X
(3) Develop and implement contingency plans	X			X
(4) Review security safeguards	X			X[2]
(5) Obtain authorizations to process	X			X
(6) Identify technical controls	X			X[2]
(7) Establish security training program	X			X[2]
(8) Develop incident reporting capabilities	X		X	
(9) Screen users	X		X	

[2] USAID reviewed security safeguards and identified technical controls for parts of the general support systems. USAID had also developed a security training program for new hires. However, the safeguards and technical controls were not identified for all sensitive systems and the training program was not adequate.

Table 2 shows the extent to which USAID's five major application systems and one general support system comply with OMB security requirements. Five of the nine requirements were selected to apply to individual application systems. The one general support system was selected because USAID is moving to an open systems environment[3] and this general support system supports the new environment. The information was obtained through interviews with program managers, system contacts, and IRM staff and reviews of documentation provided by these officials.

[3] An open system is defined as a system that can (a) exchange information through interfaces (b) change the operating system without modifications of the application system software, and (c) be used with minimal effort.

Table 2

Implementation of A-130 Security Requirements in USAID's Major Application and General Support Systems

	Major Applications Systems					General Support System
Security Requirements	**AETA**	**FACS**	**NMS**	**NAPS**	**RAMPS**	**LAN**
Assign system-level responsibility for security	No	No	No	No	Yes	No
Develop and implement security plans	No	No[4]	No	No[4]	No[4]	No
Complete a contingency plan	Yes	Yes	No	Yes	Yes	No
Review security safeguards	No	No	No	No	No	Yes
Obtain written authorization	No	No	No	No	No	No

Key:
AETA - American Electronic Time and Attendance System
FACS - Financial Accounting and Control System
NMS - New Management System
NAPS - New American Payroll System
RAMPS - Revised Automated Manpower and Personnel System
LAN - Local Area Network

[4] USAID prepared security plans in 1989. However, the plans had not been updated.

USAID Had Not Assigned System-Level Security Responsibility

OMB Circular A-130 requires agencies to assign security responsibility for each major application and general support system. Although USAID policy makes program managers responsible for assigning security responsibility for each application and general support system, managers have not done so for four of the five major application systems or for the general support system. IRM/IPA stated that the program managers are not aware of the OMB security requirements.

Specifically, USAID's policy calls for program managers to appoint information system security officers to be responsible for each automated system. The system security officer's responsibilities include conducting security awareness training for end-users, conducting annual self-evaluation reviews of the security program, and providing technical assistance to investigate security incidents. These critical functions, which should protect USAID's sensitive information, are not being performed because system security officers have not been appointed.

USAID Did Not Have Current Security Plans for Major Sensitive Systems

As required by the Computer Security Act and the OMB Circular A-130, agencies must prepare and implement security plans[5]. These plans document the security requirements of the systems and describe how the agency will meet those requirements. The plans should be revised when the system is modified. USAID policy, however, does not require preparation of security plans and USAID does not have current security plans for any of its major sensitive application systems or its general support system.

The OMB Circular directs agencies to develop security plans that address

(a) rules of behavior, (i.e. limitation of changing data);

(b) security training;

(c) personnel screening;

(d) security incidents;

(e) continuity of support or contingency planning;

(f) technical security controls, products and techniques used;

---

[5] OMB Bulletin 90-08 provides security plan guidance as required by the Computer Security Act of 1987.

(g) authorization prior to connecting with other systems;[6]

(h) protection of shared information;[7] and

(i) protection of application data when the application permits public access[8].

Although security planning is an essential element of an effective computer security program, USAID policy did not require preparation of security plans. The absence of a policy to require security planning leaves planning responsibilities unclear and leaves managers without needed guidance to implement an effective security program. Specific guidance would describe how plans will be prepared and how managers will use the plans to verify that security requirements are being met. Effective planning is essential to ensure reasonable levels of system and computer resources protection.

USAID also does not have current security plans for any of its major application systems or its general support system. To illustrate, USAID has not developed a security plan for NMS. NMS is a newly developed major application system that supports accounting, budgeting, acquisition and assistance, and operations functions. Because NMS processes sensitive financial and procurement data, it is required to follow the Computer Security Act and OMB Circular A-130 requirements. Similarly, USAID's general support system processes sensitive information and is critical to accomplish its missions in a networked environment, yet no security plan exists for this system.

USAID did prepare plans for three of the five major application systems in 1989. However, the plans were deficient and subsequent changes have made them obsolete. These plans were reviewed by the National Institute of Standards and Technology and the National Security Agency. The review concluded that the plans had significant weaknesses because, for many of the plans, vulnerability assessments were not completed, certifications were not required, and controls were inconsistent with protection needs. Additionally, the plans did not address rules of behavior, incident reporting, and any changes in assignment of security responsibilities, operating systems, physical security, and technical controls.

USAID Had Not Completed Contingency Plans

OMB Circular A-130 requires agencies to develop contingency plans for major application and general support systems. Contingency planning assures the continuity of

---

[6] Item (g) applies to general support systems only.

[7] Item (h) applies to application systems only.

[8] Item (i) applies to application systems only.

automated systems' operations by mitigating the consequences caused by unexpected loss of computer systems.

Although USAID's policy calls for contingency plans for systems, it has not implemented contingency plans for all of USAID's major systems. The lack of contingency plans for the general support system increases vulnerabilities because many application systems rely on the general support system to function. Similarly, because NMS replaces several legacy systems, USAID will rely more heavily on this system to accomplish its mission.

On a positive note, USAID has awarded a contract to provide backup for the general support system, which maintains the IBM systems. In addition, the Office of Administrative Services is developing a Continuity Of Operations Program Plan, which will address how USAID will continue operations during a crisis that renders its headquarters unusable.

USAID Had Not Conducted Application System Security Reviews

The OMB Circular directs agencies to identify system risks and vulnerabilities. Agencies should perform these reviews at least every three years. Application system security reviews are used to identify vulnerabilities in areas such as physical security, password administration, file system security, or contingency plans.

USAID policy requires system security officers and program managers to perform annual system security reviews. However, we found that USAID is not conducting application system security reviews. According to IPA staff, system contacts, and program managers, reviews have not been conducted for any of the five major application systems, including NMS. Our analysis also shows that three of the five major systems reviewed have been operating since 1989 and no security reviews have been completed. IPA staff informed us that USAID's management decided not to perform security reviews for legacy systems because they were scheduled to be replaced by NMS. Without these reviews, however, USAID is not assured that the systems are adequately protected.

USAID Had Not Implemented the Requirement to Authorize Systems to Process Data

OMB Circular A-130 requires agencies to ensure that systems are authorized to process sensitive information. Requiring an explicit management authorization to allow a system to process sensitive information is an important control to ensure that management is aware of any security vulnerabilities and accepts the responsibility if the system's data or resources are modified, lost, or destroyed. To appropriately carry out its responsibility, management needs to understand what security procedures (i.e., risk assessment, security review, contingency planning, etc.) applicable to the application or general support system have been performed and what risks and vulnerabilities exist.

USAID's policy gives the Director of IRM the responsibility to authorize this processing. However, no USAID systems had written authorizations by management to process, store, and transmit sensitive data. As a result, management has allowed systems to become operational without having explicitly considered the systems' risks and vulnerabilities. In USAID, major systems, including NMS, have been allowed to process sensitive data even though fundamental security requirements including assigning security responsibilities, developing security plans, and conducting risk reviews and application security reviews had not been performed.

USAID Had Not Fully Defined Technical and Security Control Requirements

To safeguard automated information systems, OMB's Circular A-130 directs agencies to ensure that technical and security controls are identified, built, and used within application and general support systems. To meet the OMB requirement, agencies should develop guidelines that describe the protective measures that should be considered for various types of systems. Using the guidelines, agencies then determine what controls should be applied to individual systems. The guidelines also provide a basis to measure the extent to which controls have been successfully incorporated in sensitive systems.

USAID's policy requires systems to have adequate technical controls to protect personnel, information, and system resources. However, IRM had not provided guidelines describing what technical controls should be included in sensitive application systems. IRM did prepare draft security guidelines that support the implementation of technical security measures for USAID's application systems. These included controls and guidelines for application systems and an agency-wide security architecture. IRM staff stated that USAID's process to disseminate the guidelines is the Automated Directives System (ADS) and these guidelines do not fit the format required by ADS. Therefore, the guidelines were not distributed. Without these guidelines, system managers do not know what technical controls should be considered and implemented for application systems.

IRM did develop and distribute technical guidelines for parts of USAID's general support system.

USAID's Computer Security Training is Inadequate

The Computer Security Act of 1987 and OMB Circular A-130 require agencies to conduct training in computer security awareness and accepted computer security practices. Adequate security training is needed so that individuals can perform their assigned security responsibilities. Such training should include physical security, hardware security, personnel, risk management, vulnerability assessments, and security and contingency planning. USAID's policy calls for security training for system security

officers, program managers, and users. However, USAID's program did not appear adequate to provide the tools to understand how to implement an effective security program. We interviewed 13 program and system managers and found that 7 were not familiar with security terminology or aware of their security responsibilities. Three of the nine program and system managers interviewed believed that IRM was responsible for the security of their systems rather than themselves.

USAID Lacks Reasonable Assurance That Sensitive Information and Resources are Protected

USAID's failure to follow key security requirements exposed USAID to unacceptable risks that resources will not be adequately protected from fraud or misuse, and that sensitive data and systems will not be adequately protected from loss or destruction. Specifically, USAID's systems may be operating at unacceptable levels of risk, may have inadequate safeguards incorporated, and may not be prepared to continue operations should events occur that prevent normal operations.

USAID is not alone in this situation. GAO has cited inadequate security programs at most of the agencies it has evaluated for compliance with security requirements, including 10 of the 15 largest federal agencies.[9] The GAO report also highlights the importance of an effective security program in an environment that increasingly relies on computers to conduct agency business. GAO cited several instances of improper use of systems that put billions of dollars of assets at risk of unauthorized disclosure, loss, or modifications. Increased threats and vulnerabilities reported by GAO include:

- Increasing number of attacks by intruders who have successfully shut systems down and corrupted sensitive data.
- Unprotected personal data manipulated for individual gains.
- Systems vulnerable to loss or misuse because of excessive access privileges.
- Individuals making unauthorized changes to computer programs to receive improper payments.
- Unauthorized users performing unauthorized activities without being traced.
- Individuals sabotaging or congesting networks with malicious code or virus.

---

[9] Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996)

GAO has also identified information security as one of twenty government wide areas that carry a high risk because of the value of assets that are vulnerable to fraud, waste, or abuse.[10]

USAID is similarly vulnerable because it processes billions of dollars of federal funds on systems that have not been developed or operated to ensure effective security. Three examples illustrate the threats and vulnerabilities faced by USAID's automated systems.

First, by gaining knowledge of USAID's processing procedures and taking advantage of an inadequate computer security environment, USAID's public network, which is outside the firewall protecting USAID's sensitive systems, was attacked by an internet hacker in December 1996. Although this attack was outside the firewall and involved non-sensitive systems, USAID's resources were consumed to investigate the incident, analyze the vulnerabilities, disconnect the public system, and develop security recovery procedures. Further, disconnecting the system made resources unavailable to USAID employees, disrupting USAID operations.

Second, in March 1997, we reported deficiencies in NMS access controls that indicate that USAID lacks reasonable assurance that NMS provides adequate safeguards to prevent: (1) diversion of funds for personal financial gains and (2) inappropriate access to sensitive financial, procurement, or privacy protected data.[11] In one case, we identified that users with view roles (a type of system access that allows users to see the data but not to change the data) could actually change vendor financial data. We reported that if users could make unauthorized changes to vendor or bank information, an unscrupulous user could change the vendor address and the bank to which payments are to be made, creating a risk that payments could be fraudulently diverted. Although this problem had been identified in October 1996, it had not been corrected when we completed audit work in March 1997. In another case, we found that users were allowed to enter and change any data within a broad organizational unit. In this case, one mission reported that it had already encountered an instance of an unknown user entering unauthorized data. Finally, we reported that users could be assigned conflicting roles that circumvent appropriate separation of duty requirements. For example, a single user could be assigned the role of Accounts Payable Authorized Certifying Officer and Funds Control Miscellaneous Obligation Approver, two incompatible duties.

Third, we analyzed problems reported by NMS users (called the help desk database). Between January 2, 1997 and August 7, 1997, users reported 2,893 problems. Our review of 987 problems found 7 reports of NMS security vulnerabilities. For example, in several cases, software changes made to correct a problem affected users' access to the

---

[10] High Risk Series: Quick Reference Guide (GAO/HR-97-2, February 1997).

[11] Audit of the Worldwide Deployment of the New Management System (NMS) (Report No. A-000-97-004-P, March 31, 1997)

system. In one case, unsynchronized database tables caused the automatic assignment of additional roles to some users.

To USAID's credit, when we discussed NMS security weaknesses with its officials, they took immediate steps to begin addressing the deficiencies. Management drafted a statement of work requesting contract services to conduct a security assessment of NMS and committed to bring the system into compliance with the security laws and regulations.

USAID Lacks Management Controls to Implement an Effective Security Program

These security deficiencies existed because USAID has not implemented effective management controls to meet the requirements of the Computer Security Act of 1987 and OMB Circular A-130. Specifically, USAID had not: (1) developed an organizational structure that clearly delegates responsibility and provides appropriate authority, (2) established planning policies that provide an essential framework for an effective security program, and (3) implemented key management processes to ensure that security requirements are met. The underlying cause of the lack of management controls is that top management had not supported an effective security program.

Organizational Problems

In March 1997, we reported that the IRM office did not have the authority to manage information resources and enforce data or system development standards.[12] The office also lacked the authority to implement an effective security program or monitor compliance with security requirements. An appropriate organizational structure is an essential component of an effective system of management controls. Fragmented and unclear responsibilities and the fact that no organization had the authority to enforce security requirements is, we believe, a primary reason that USAID's security program deficiencies existed.

USAID's delegation of responsibilities and authority for security was fragmented, and in some cases, unclear. Responsibilities were dispersed throughout USAID, yet when we discussed security roles with responsible officials, many were not certain of their roles or responsibilities.

Attempts to identify the organization responsible for security controls in NMS illustrates these problems. No security plans, security reviews, or authorizations to process were completed for the NMS system. When we tried to talk to the responsible official about

---

Audit of Worldwide Deployment of the New Management System (Report No. A-000-97-004-P, March 31, 1997).

these deficiencies, senior USAID managers referred us to officials on the NMS Task Force–the organization responsible for developing NMS. Task force officials, claiming that the task force did not have responsibility for NMS security, noted that IRM/IPA was responsible for NMS security. The then Acting Director of IRM confirmed that IRM/IPA did not have responsibility for NMS security requirements, explaining that senior USAID executives directed that IRM/IPA not be involved in developing NMS security requirements.

IRM/IPA officials also explained that they did not have authority to implement other aspects of the security program. For example, although they provided security training, they did not have the authority to require employees from other organizations to attend the training. As a result of this lack of authority, IRM/IPA interpreted their responsibility as limited to promulgating policies. They believed that under current circumstances, program managers have the responsibility to ensure an effective security program in their area of responsibility. In fact, program managers did have significant responsibility. However, the majority of program managers we talked to were not aware of their responsibilities, and stated that IRM/IPA was responsible for security.

Limited resources also appear to be a factor. According to OMB Circular A-130, officials assigned security responsibility must be knowledgeable in security and the supporting technologies. USAID's security program is accomplished through two direct-hire employees–the USAID security officer, a permanent focal point for security issues, and the alternate security officer. These officials provide overall direction to contractor personnel. These officials and other IRM senior managers pointed out that these resources were too limited to support a comprehensive security program. In addition, these officials recognize that they did not have the technical security knowledge called for by OMB Circular A-130. They noted that the security officer position had been subject to significant turnover at USAID, and USAID currently does not have people with specialized computer security skills.

Planning Deficiencies

The lack of a policy for security planning was also a significant cause of the computer security deficiencies because the planning process establishes the framework needed to implement an effective program. Among other things, the planning process provides the foundation for ensuring that threats and vulnerabilities are analyzed, security controls are designed into systems, and an effective system is in place to monitor compliance with security requirements. For example, security plans would identify the technical controls needed to protect systems and data from specified threats.

Without adequate planning, USAID cannot effectively enforce security policies and procedures. To illustrate, because USAID did not require plans to identify and specify technical controls, it did not have a basis to monitor the extent to which these controls have been implemented and remain effective.

Disciplined Management Control Processes Needed

OMB Circular A-130 requires agencies to establish and maintain processes to manage information throughout its lifecycle. USAID, however, has not implemented effective management control processes to ensure that: (1) computer security is addressed throughout the system's lifecycle, (2) security policies and procedures are enforced, and (3) adequate resources, including qualified and experienced staff, are devoted to the security program.

These processes establish a workflow to comprehensively address how an agency identifies sensitive systems, prepares security plans, determines the appropriate security controls, ensures that they are built into the system life-cycle, assesses the effectiveness of the design and implementation of security controls, and obtains management's authorizations to allow systems to process data. OMB Circular A-130 and OMB Bulletin No. 90-08 require agencies to establish these management control processes. For example, the Bulletin requires agencies to obtain independent advice about the adequacy of security plans, and to ensure that systems are reviewed when the operational environment changes.

In part, USAID's implementation of management processes was impeded by the lack of disciplined IRM processes, including a system life cycle methodology. A disciplined life-cycle methodology requires that security controls be incorporated in the development process and assessed throughout the life of the system. In response to our March 1997 report citing technical and operational deficiencies in NMS, USAID agreed to implement a disciplined system methodology.

Top Management Support Needed

The underlying reason that USAID had not implemented an effective system of management control, and therefore, had not implemented an effective computer security program is that senior managers did not recognize the importance of protecting computerized information or provided the necessary level of support. The lack of attention to date was illustrated both by the deficiencies highlighted in this report and by the lack of effective management controls. Although USAID is not alone in its limited support for computer security activities, GAO's identification of computer security as a government-wide high risk area highlights its growing importance as an area deserving top management attention.

The lack of effective computer security provisions in developing NMS provides a case study in the lack of management support. OMB Circular A-130 makes the USAID Administrator responsible for implementing an effective computer security program. The Circular requires heads of agencies to oversee, evaluate, and periodically review IRM activities for conformity with policies established in the circular. The Administrator

delegated responsibility to a senior management official. However, several officials told us that computer security requirements were not met during the development of NMS because the responsible official determined that incorporating security requirements would delay deployment of the system. Rather than viewing security as an important capability that needed to be incorporated into the system, top management appeared to have viewed security as an impediment to meeting its schedule.

The OMB Circular further calls for agencies to consider identifying computer security weaknesses as a material deficiency in their annual reports to the President and Congress on the status of internal controls if there is: (1) no assignment of security responsibility, (2) no security plan, or (3) no authorization to allow a system to process data. The annual report identifies material internal control deficiencies pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act.

Conclusion

Because of the increased reliance on automated systems to conduct and manage finances and operations, and the increased threats identified by GAO, an effective computer security program is essential. An effective computer security program, however, requires disciplined processes which include an effective system of management controls including, an appropriate organizational structure and planning process. A recognition by top management of the importance of computer security and a commitment to correct current deficiencies is essential if USAID is to adequately protect sensitive data and systems from unauthorized access, disclosure, and loss.

Recommendations

We recommend that the Acting Assistant Administrator for Management demonstrate support for an effective computer security program by taking action to:

Recommendation No. 1: Appoint a senior manager, reporting to the Chief Information Officer, to be responsible for implementing an effective computer security program and provide the manager the authority and resources needed to do so.

Recommendation No. 2: Direct the computer security program manager to develop and implement an effective computer security program by:

2.1 Clarifying organizational roles, responsibilities, and authorities.

2.2 Ensuring that adequate resources and skills are available to implement the program.

2.3 Revising policies to incorporate a planning process that will provide a sound foundation for an effective computer security program.

2.4 Implementing disciplined processes to ensure compliance with the Computer Security Act of 1987 and OMB Circular A-130.

2.5 Bringing sensitive computer systems, including NMS, into compliance with computer security requirements by (1) assigning security responsibility, (2) preparing security plans, (3) completing contingency/disaster recovery plans, (4) identifying technical controls, (5) conducting security reviews, and (6) obtaining management's authorization before allowing systems to process data.

Recommendation No. 3: Identify computer security deficiencies as a material internal control weakness in USAID's annual Federal Managers' Financial Integrity Act report.

MANAGEMENT COMMENTS AND OUR RESPONSE

In a September 26, 1997 response to our draft report, the Acting Assistant Administrator for Management (AA/M) concurred with the three recommendations and stated that USAID is taking action to hire a senior manager who will be responsible for implementing an improved security program. The response also noted concerns related to the security program in aggregate. Based on our review of the response, we revised the report to clarify the meaning of the specific issues raised. We believe that the report accurately describes USAID's security deficiencies and have attached in its entirety USAID's response to the draft report.

SCOPE AND METHODOLOGY

Scope

Our review of USAID's compliance with the Computer Security Act of 1987 and the revised OMB Circular A-130 was limited to an analysis of USAID's policies and procedures covering security of sensitive systems and data as defined in OMB Circular A-130. Thus we did not analyze the adequacy of agency-wide security controls that are in place or controls over classified national security information. Our coverage was limited primarily to the five major sensitive systems identified by USAID–American Electronic Time and Attendance System, Financial Accounting and Control System, New American Payroll System, New Management System, and Revised Automated Manpower and Personnel System; and the general support system. Our review was conducted at USAID/Washington between May 1997 and July 1997 in accordance with generally accepted government auditing standards.

During the course of the review, we did raise a question about our independence because USAID's Automated Directives Systems appeared to assign some monitoring responsibilities to the Office of Security which is part of the Office of the Inspector General. Because the Office of Security and the Office of Audits both report to the Inspector General, a monitoring role for the security office could raise questions about our organizational independence, based on the second general standard of the generally accepted government auditing standards[13]. However, when we discussed the issue with security and IRM officials, it became clear that the Administrator had not delegated responsibility to the security office for overseeing sensitive information. The security office's responsibilities are limited to overseeing classified national security information. Therefore, we concluded that our independence was not affected.

[13] Independence, the second general standard, requires that the assigned auditor or team is independent in attitudes, beliefs, and there is no appearance of a conflict of interest.

In response to our draft report, the Acting Assistant Administrator for Management's (AA/M) raised the question of whether the USAID's vulnerabilities were accurately assessed because we did not evaluate the implementation of security controls in AID/Washington or the missions. We agree that we did not evaluate the implementation of security controls and therefore, did not conclude that the vulnerabilities described were the results of not meeting the applicable federal laws and circular. The examples were provided to show that failure to practice the key security requirements can lead to the vulnerabilities described in the report.

Methodology

For this review, we used the Computer Security Act of 1987 and the OMB Circular A-130 as the mandate for USAID to establish and implement computer security requirements. We then compared USAID's policies and procedures to those requirements to determine the extent to which USAID has incorporated the policies and procedures in its security program.

To accomplish this, we determined USAID's practices in meeting the nine security requirements identified by OMB. We also analyzed five major application systems and the telecommunications network general support system. We selected these systems based on USAID's identification of its major systems and compared the system to five of nine OMB requirements that were applicable to specific application systems.

We interviewed USAID's Information Resource Management, Administrative Services, contractors, systems contacts, and managers to gain an understanding of security policies, procedures, and practices. In addition, we interviewed officials from the National Institute of Standards and Technology to obtain better understand current best practices regarding security planning and training.

We also reviewed available documentation describing how USAID implemented security requirements agency-wide and for each system. We examined USAID's security policies, procedures, and related security documents for protecting automated systems, such as the Automated Directives Systems (ADS) Chapters: 551–Automated Information Systems Security and 531 Continuity of Operations Program; Handbook 6–Security and Personnel Security Program; Draft Strategic Information Resources Management Plan; and Draft Security Architecture. We also reviewed reports by the Information Policy and Administration Division and GAO.

U.S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

SEP 26 1997

MEMORANDUM

TO: AIG/A, Everette B. Orr

FROM: A-AA/M, Richard C. Nygard

SUBJECT: Audit Report # A-000-97-008P

The subject audit makes three recommendations in response to its findings that USAID has not implemented an effective security program that meets the requirements of applicable federal laws and circulars. USAID concurs in the recommendations.

A number of statements in the audit incompletely represent the status of and facts related to the computer security program at USAID in aggregate. A number of instances referenced in Attachment (1) offer information related to this concern.

In my capacity as Acting USAID Chief Information Officer, I have authorized the hiring of a senior manager responsible for implementing computer security program improvements.

The staff of M/IRM assigned to computer security are dedicated public servants. These personnel and their management are committed to making the USAID computer security program a model for the federal government. Attachment (2) lists accomplishments of this team which were overlooked in presentation of report findings.

Attachments: a/s

320 TWENTY-FIRST STREET, N.W., WASHINGTON, D.C. 20523

Attachment (1)

1. There was no audit objective or audit activity to evaluate implementation of security controls in AID/W or in the missions. Analysis of the computer security program without this information is an incomplete representation of the issue and raises the question whether the vulnerability of the agency can be accurately assessed limited to the findings of the report.

2. Every hacker incident is serious and protection against negative impact is essential. Yet analysis of USAID vulnerabilities as framed in this audit report may lead to inappropriate conclusions from the information reported. The bulk of the audit addresses essential action for sensitive systems. The hacker incident reported was on a public network on non-sensitive information, outside the firewall protecting critical systems of the agency. Casual investigation or reading of the report could conclude that all USAID systems are under equal risk from hackers as a result of this regrettable incident.

After searching our records we were unable to determine any instances of deliberate and malicious compromise of sensitive information which call for the special protection addressed in A-130 and the Computer Security Act of 1987.

3. Applications security assessments have been limited at USAID. Routine assessments are conducted on general support systems including local area network servers, Unix minicomputers and the IBM mainframe. As a consequence the introductory paragraph including the second sentence which states "has not implemented .... assessing systems to ensure they are protected," is inaccurate. To be true this statement requires context and further description of security implementation actions which are in effect.

4. Table #1 of the report states that USAID has no implementation of the A-130 security training program requirement. M/IRM conducts computer security awareness training for all new hire employee the day of arrival.

5. Table #1 of the report also states that USAID has no review of security safeguards or identification of technical controls. In fact, the USAID computer security program has issued security standards for local area networks and Unix systems, against which audits are conducted both in Washington and the field during mission assessments. As presented the tabular references are misleading to the reader who might conclude that no security exists for any USAID system.

M/IRM/IPA
Information Systems Security

Selected Accomplishments FY 1996/97

- **Information Systems Security Policy/Procedures**

  Developed USAID Information Systems Security Policies and Procedures i Handbook 18

  Updated and Converted Handbook 18 Security Policies and Procedures to ADS, Section 551, Automated Information Systems Security

  Developed USAID's Sensitive But Unclassified (SBU) Information Protection Policy

  Currently Developing USAID's Remote Connectivity Security Policy

  Developed USAID's Information Systems Security Architecture Document (Update Scheduled)

- **FY 97 Security Awareness Training**

  Conducted 25 New Hire Security Training Sessions (over 500 employees)

  Presented 3 Security Briefings at the USAID System Managers Conference

  Conducted E-Mail/SBU Security Briefings for All USAID/W Personnel as Directed by the Administrator

  Designed/Developed the Agency's Information Systems Security Web Page as a Form of Security Awareness

- **Security Evaluations and Audits**

  USAID's Internet Firewall (several times per year)

  20 LAN Servers in USAID/W

  Remote Scans and Audits of AIDNET UNIX Systems Worldwide (165.13 net)

  Remote Scans and Audits of AIDNET UNIX Systems Worldwide Communicating via VSAT (206.118 net)

  NMS LAN Support Servers at the NMS Development Site

  The NMS Configuration Management UNIX System

  USAID's Public Internet Servers (the 198.76.84 net)

  IBM Mainframe (Audit of the Validity of Application Systems User Accounts -- in process)

  USAID's E-mail System (Banyan's BeyondMail System)

- **Security Incident Response**

  Assisted Network/System Managers with Recovery Procedures after the "Blue Elf" Hacking Incident on USAID's Public Network

  Frequently Respond To Computer Virus Infections in USAID/W and Mission Systems

  Responded to, Investigated, and Reported on the Recent Cable Room Security Incident

  Investigated Several Unsuccessful Attacks on USAID's Private Network behind the Firewall

- **Research and Evaluation of Security Products**

  Public-key Encryption Products for Safeguarding SBU Information

  Firewall Security Systems

  Remote User Advanced Authentication Systems

  Antivirus Packages for Use with Windows 95

  Antivirus Packages for Use on LAN servers

  Internet, Intranet, System, and Web Server Security Scanning Tools

  Encryption Solution for Secure E-mail Between Mission/Khartoum and Mission/Nairobi

- **FY 97 Ad Hoc Security Tasks**

  Completed Over 125 Ad Hoc Security Tasks for USAID/W Offices and USAID Missions, e.g.,

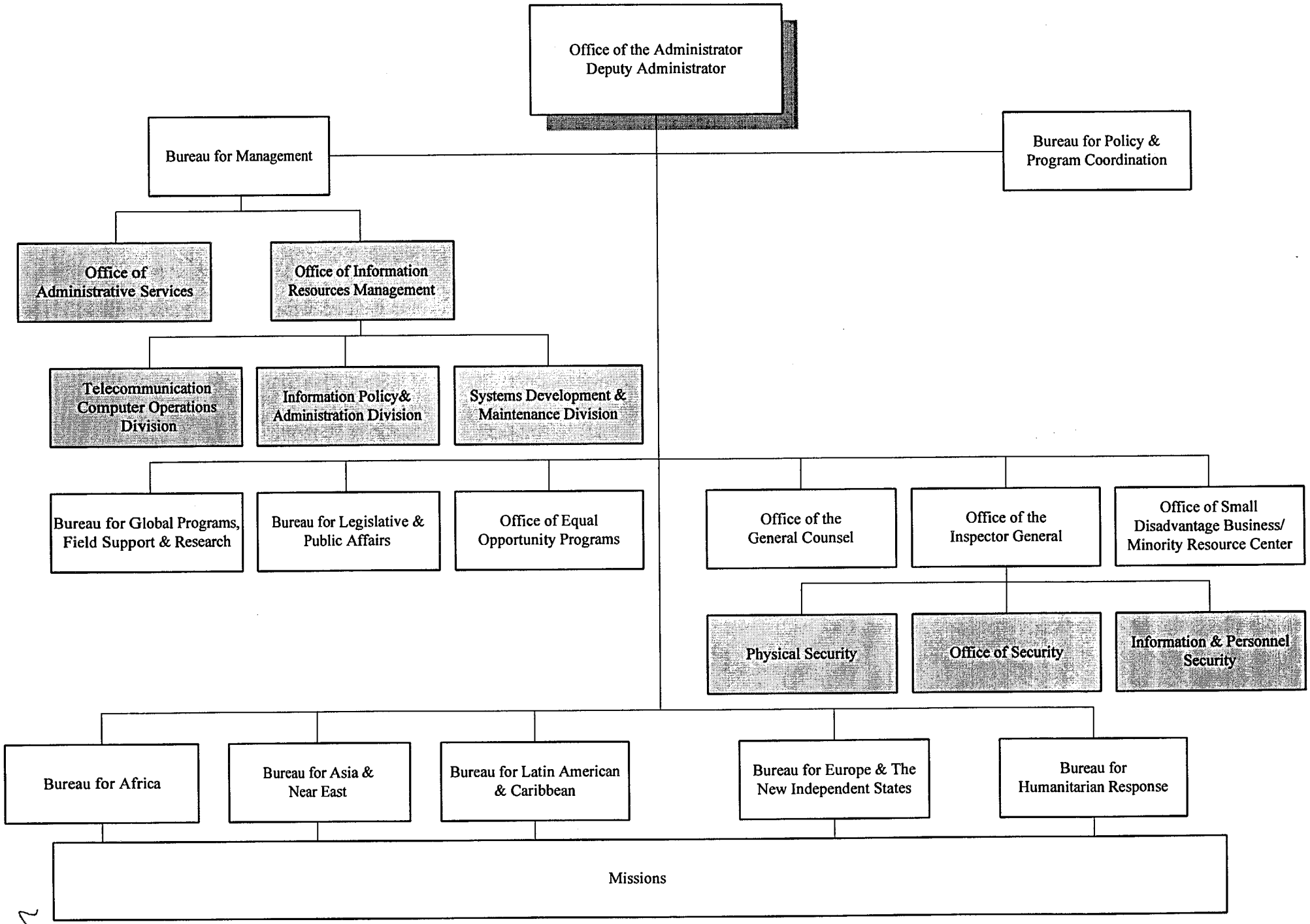
  Detecting/Removing Computer Viruses
  Handling Computer Virus Hoaxes
  Responding to Suspected Intrusion Attempts by Hackers
  Addressing Remote Connectivity Security Issues
  Advising Missions on Encryption and Other Security Products
  Interpreting USAID IT Security Policies
  Advising Users on Classified Processing Requirements
  Contingency Planning Consultation to Missions

- **Security Systems Management and Operation**

  USAID's Checkpoint Firewall in the RRB

  USAID's V-One Remote User Advanced Authentication System

ORGANIZATIONAL SECURITY RESPONSIBILITIES



APPENDIX III

Glossary

Availability	Protection against denial of service, to include errors, damage, destruction, loss, or other events that may affect continuity of systems operations.
Certification	A technical evaluation of a sensitive system to see how well it meets the security requirements.
Computer Security	Safeguards applied to computers, hardware, programs, data, and facilities to assure availability, confidentiality, and integrity.
Confidentiality	Protection of sensitive system against unauthorized disclosure.
Firewall	A method of protecting connected networks from break-in by unauthorized outsiders.
General Support System	An interconnected set of information resources (hardware and software) under the same direct management control which shares common functionality (i.e. data processing or network). For example, a local area network is a general support system.
Integrity	Protection against unauthorized accidental or malicious modifications.
Major Application System	A system using information technology to satisfy a specific set of user requirements requiring special management attention to security.
Security Plan	An overview of the systems' security requirements and the agency's plan for meeting those requirements. OMB has provided specific guidelines for preparing these plan (OMB Bulletin No. 90-08).
Technical Controls	Controls incorporated into systems to achieve the goals of availability, confidentiality, and integrity. These controls are supported by the operating system, database management, or network operating systems. Examples of technical controls are encryption, variance detections, auditing capabilities, user identification and verification, and data validation.