

GAO

November 1988

ARMS CONTROL AND
DISARMAMENT
AGENCY

Better Controls Are
Needed to Protect
Classified Information



About Our New Cover . . .

The new color of our report covers represents the latest step in GAO's efforts to improve the presentation of our reports.

National Security and
International Affairs Division

B-212009

November 10, 1988

The Honorable Dante B. Fascell
Chairman, Committee on Foreign Affairs
House of Representatives

The Honorable William S. Broomfield
Ranking Minority Member
Committee on Foreign Affairs
House of Representatives

You requested us to review the extent to which the Arms Control and Disarmament Agency (ACDA) complies with statutes, executive orders, regulations, and other applicable standards governing the protection of classified documents. This report transmits the results of our review of ACDA's safeguarding of national security information. As agreed with your offices, we provided separate reports on ACDA's sensitive compartmented information facility (SCIF) for storage of compartmented (codeword) information and on allegations of security breaches by an ACDA employee and subsequent investigations.¹

ACDA does not control national security, or classified, information in compliance with applicable standards at its Washington, D.C., headquarters or at its negotiating offices in Geneva, Switzerland.

- ACDA does not have an adequate Top Secret control system. At its headquarters, ACDA could not locate all the Top Secret documents for which it is responsible; its records were inaccurate, incomplete, and out of date, and it had not completed annual inventories of its Top Secret holdings. In Geneva, ACDA had not appointed a Top Secret control officer and had no system for controlling Top Secret documents.
- ACDA has not complied with regulations for physical protection of classified information. Top Secret, codeword, and other documents were stored in unauthorized safes and areas. Daily close-of-business security checks were not always done, safe combinations were not changed, and classified documents were improperly marked. ACDA also did not have up-to-date records on its safes and could not locate 62 headquarters safes.

¹Arms Control; Improvements Needed to Protect Compartmented Information (GAO/NSIAD-88-216, Aug. 24, 1988) and letter dated August 10, 1988.

The Information Security Oversight Office,² which monitors government-wide implementation of procedures to safeguard national security information, has also identified weaknesses in several areas of ACDA's information security program. In its three inspections of ACDA in 1984, 1985, and 1986, the Oversight Office found poor control over Top Secret documents, a history of incomplete Top Secret inventories, a lack of thorough investigations into unaccounted for Top Secret documents, and documents improperly marked. In addition, the Oversight Office reported other weaknesses, including improper classification of documents and inadequate security education.

In its 1986 inspection report, the Oversight Office made recommendations aimed at improving all aspects of ACDA's information security program. These included increasing ACDA staff familiarity with proper classification and safeguarding procedures through a security education program, developing and implementing a security inspection plan, and rigorously enforcing security regulations and procedures. At the time of our review, ACDA had not implemented the Oversight Office's recommendations to address weaknesses in its information security program.

We discussed our findings with the Deputy Director, ACDA, and other cognizant officials. In May 1988, ACDA began to take corrective action to address some of the deficiencies in its information security program. In a May 2, 1988, memorandum to all ACDA staff, the Director of ACDA stated that security is to be an agency priority. As a first step toward establishing accountability for Top Secret documents, ACDA's Deputy Director requested that each headquarters bureau and office conduct a thorough review of its files, inventory its Top Secret holdings, and ensure that documents were properly stored.

According to the Security Officer, ACDA is also updating its files on the number and locations of safes in its Washington, D.C., offices. ACDA has asked each bureau to provide current information; however, it has not devised any specific approach to locate or otherwise explain the 62 headquarters safes it could not account for and assess the potential security risk.

²The Information Security Oversight Office is an administrative component of the General Services Administration that receives its policy direction from the National Security Council.

Conclusions and Recommendations

Because ACDA had not fully implemented minimum security requirements or acted on the Oversight Office's recommendations regarding information security, ACDA could not ensure that it has control over all its classified material. ACDA had not provided adequate control systems, oversight, and enforcement to ensure compliance with requirements.

Although ACDA has recently begun corrective action, more should be done. ACDA management needs to make a commitment to effective information security and ensure its staff adhere to regulations. Accordingly, we recommend that the Director, ACDA, take the following actions:

- Implement and enforce existing regulations to ensure proper handling, control, and accountability of Top Secret, codeword, and other sensitive documents, including appointing a Top Secret control officer for Geneva, developing control procedures for all ACDA and delegation staff in Geneva, and establishing procedures to ensure that Top Secret document information is recorded in a timely and accurate manner.
- Conduct an inventory of all Top Secret documents in ACDA's possession at both Washington and Geneva to determine what ACDA should be accountable for and identify what documents may be missing. If documents cannot be accounted for, report the documents to the originating agency so that an assessment can be conducted to determine if security was compromised.
- Account for the safes that are on ACDA records but not located in ACDA. Develop and maintain accurate records regarding the location of safes approved for storage of classified information.
- Enforce regulations to ensure the physical protection of classified information, including meeting storage requirements, changing lock combinations, and taking basic security precautions such as checking safes at the close of business, and marking documents properly.
- Act on the Information Security Oversight Office's recommendations for improving ACDA's information security program, including security education programs, self inspections to ensure proper storage, and adherence to classification regulations.

Agency Comments

We requested comments on a draft of this report from ACDA, the Information Security and Oversight Office, and the Department of State. ACDA concurred with our conclusions and recommendations (see app. II), and the Department of State had no comments (see app. IV). The Oversight Office stated our findings were consistent with its own observations. The Oversight Office suggested a few minor changes for clarification, which we incorporated where appropriate (see app. III).

Our work was conducted in accordance with generally accepted government auditing standards. Appendix I contains detailed information on our findings and a discussion of our objectives, scope, and methodology.

As arranged with your offices, we plan no further distribution of this report until 2 days from its issue date. At that time we will send copies to the appropriate congressional committees; the Director of the Arms Control and Disarmament Agency; the Secretary of State; the Director, Information Security Oversight Office; the Director of Central Intelligence; the Director, Office of Management and Budget; and other interested parties.

This report was prepared under the direction of Joseph E. Kelley, Associate Director. Other major contributors are listed in appendix V.



Frank C. Conahan
Assistant Comptroller General

Contents

Letter		1
Appendix I		8
ACDA's Control and Protection of Classified Documents Needs Improvement	Background	8
	Objectives, Scope, and Methodology	9
	ACDA Does Not Have an Adequate Top Secret Document Control System	10
	ACDA Does Not Fully Comply With Standards for Physical Protection	13
	ACDA Has Begun Corrective Actions	17
Appendix II		18
Comments From the Arms Control and Disarmament Agency		
Appendix III		19
Comments From the Information Security and Oversight Office		
Appendix IV		20
Comments From the Department of State		
Appendix V		21
Major Contributors to This Report	National Security and International Affairs Division, Washington, D.C.	

Abbreviations

ACDA	U.S. Arms Control and Disarmament Agency
GAO	U.S. General Accounting Office
NODIS	No Distribution
OADR	Originating Agency's Determination Required
SCIF	Sensitive Compartmented Information Facility

ACDA's Control and Protection of Classified Documents Needs Improvement

The Arms Control and Disarmament Agency (ACDA) is the central organization in the U.S. government for the formulation and implementation of arms control policy, as established by the 1961 Arms Control and Disarmament Act (22 U.S.C. 2551). ACDA carries out its responsibilities at its Washington, D.C., headquarters and its Geneva, Switzerland, offices with a staff of about 250, including approximately 50 detailees from the Departments of State and Defense.

As a part of its mission, ACDA handles classified information, both internally generated and received from external sources. Thirty-five percent of the documents we reviewed in Washington, D.C., were classified, while about 65 percent in Geneva were classified. We reviewed ACDA's security procedures to determine whether ACDA had protected classified material as required by regulations. We found that ACDA had not complied with regulations designed to protect classified material from unauthorized disclosure.

Background

Executive Order 12356 prescribes a uniform system for classifying, declassifying, and safeguarding national security information. The order and the Information Security Oversight Office's Directive 1, which implements the order, establish minimum standards for protection of classified information. They specify that agencies must protect classified information commensurate with the degree of damage that could be caused to national security by unauthorized disclosure. The order and directive require that information classified Confidential or Secret be protected by physical safeguards, although there is no requirement for keeping individual records on such documents. However, Directive 1 requires that agencies account for all Top Secret documents through a system that provides for controlled access and annual physical inventories. Some national security information, regarded as especially sensitive, is divided into categories, or compartments, to limit access. Known as sensitive compartmented information, or codeword, such information must be provided extra protection in control and storage. The Director of Central Intelligence is responsible for establishing and enforcing these controls.

ACDA's implementing regulations are the same as those adopted by the Department of State, the U.S. Information Agency, the Agency for International Development, and the Overseas Private Investment Corporation. These joint uniform regulations establish more stringent requirements for storage of classified information at overseas posts.

Specifically, Top Secret information, as well as codeword, must be stored in a vault.

Objectives, Scope, and Methodology

Our objective was to determine the extent to which ACDA complies with executive orders, regulations, and other applicable requirements governing the protection of national security information. To identify the minimum requirements regarding classified information, we examined Executive Order 12356, which outlines the basic framework for classifying, declassifying, handling, and protecting classified data, and the implementing federal regulation, Directive 1 (32 CFR 2001). We analyzed ACDA's security procedures to determine the degree to which they address and implement the Executive Order and regulations' general guidelines.

We reviewed previous internal and external reports on ACDA's security procedures, including reports by the Information Security Oversight Office, which is charged with monitoring government-wide the implementation of procedures to safeguard national security information. We interviewed the senior program analyst in the Oversight Office who conducted the three most recent reviews of ACDA's information security program (1984 through 1986).

We conducted physical inventories of ACDA safes to verify ACDA's records on the number and location of containers approved for storage of classified information. We examined the contents of 60 out of a total of 1,721 safe drawers in ACDA's Washington, D.C., and Geneva, Switzerland, offices to determine whether ACDA had complied with applicable regulations on accounting for, storing, and marking classified documents. Of these safe drawers, 41 were randomly selected and 19 were judgmentally selected.

In addition, we randomly selected a sample of 153 documents from 1,601 active documents listed on ACDA's Top Secret control log as of November 1987 to verify the accuracy of the information and determine whether ACDA could account for them. Because this sample indicated problems in ACDA's Top Secret control records, we also examined the remaining 1,448 log entries for similar weaknesses. We did not attempt to account for documents classified below Top Secret, because ACDA does not require separate record-keeping for these documents.

We interviewed officials from each of ACDA's four operating bureaus and four staff offices as well as other ACDA staff regarding the security procedures they followed in both Washington and Geneva.

Our work was conducted from August 1987 to April 1988 in accordance with generally accepted government auditing standards.

ACDA Does Not Have an Adequate Top Secret Document Control System

ACDA's records of its Top Secret documents in Washington, D.C., were inaccurate, incomplete, and out-of-date, and, in Geneva, ACDA had not appointed a Top Secret control officer and had no system for controlling Top Secret documents. Thus, ACDA cannot ensure that it can account for all Top Secret documents.

Directive 1 requires that agencies designate a Top Secret Control Officer to maintain control and accountability for all Top Secret material, including maintaining a permanent register to account for all documents and conducting yearly inventories. ACDA's Top Secret Control Officer is located in the Office of Administration, Communications and Services Section, an office primarily responsible for administrative support in supply and communications. ACDA's Administrative Director has oversight responsibility for the Top Secret Control function.

The Top Secret Control Officer, who is also the Chief of the Communications and Services Section, did not personally perform the Top Secret control duties prescribed by the regulations. He had delegated these duties through the Mail and File Supervisor to a File Clerk. We found no evidence that the Top Secret Control Officer had instituted procedures to ensure that the control duties had been performed.

Although ACDA has established procedures for handling and controlling Top Secret documents at its Washington headquarters, it has no mechanism to ensure compliance with them. According to the procedures, all Top Secret documents are supposed to be submitted to the Top Secret Control Officer, who should record each document in a log, assign a unique number, and record other information such as the individual responsible for the document. Document transfers, downgrades, and destruction information should also be recorded on the log.

Clerical and substantive errors in Washington's Top Secret control log make it unreliable as a basis for establishing accountability for Top Secret documents. Our random sample of 153 documents selected for verification from the 1,601 entries on the active document log included

eight (5.2 percent) documents that should not have appeared on the log because they had been destroyed, downgraded from Top Secret, or sent to storage. These actions were recorded in manual files but had not been entered into the automated log or had been entered incorrectly. According to ACDA officials, they did not have data verification procedures to ensure that document control information is entered in a timely and accurate manner.

ACDA could not locate a total of 86 Top Secret documents that we requested in its Washington office: 5 from our random sample and 81 from further review of the remaining log entries. ACDA's Top Secret Control Officer told us that 2 of the 5 documents from the random sample had been sent to the federal records center, but they were not in the designated storage location there, and two had been signed out to former employees. According to the ACDA employee responsible for the fifth document, he had reported the document missing in 1976, but ACDA's records did not reflect that status. Of the additional 81 documents that ACDA's Top Secret Control Officer could not locate, 47 had been signed out to former ACDA employees, 7 document records contained no information on the persons responsible, and 27 documents had been signed out to individuals on a temporary basis between 1982 and 1984 and had not been returned to the Top Secret Control Officer for control or disposition.

As of July 1988, ACDA had not recovered all of the documents it could not account for. It had not taken steps to report missing documents to the originating agency so that a damage assessment could be conducted. According to the Information Security Oversight Office, which conducts yearly reviews of ACDA's information security program, ACDA has not conducted thorough investigations of missing documents in recent years. In its 1985 report, the Oversight Office criticized ACDA's practice of "writing off" as lost documents it could not account for.

ACDA Staff Did Not Always Report Possession of Top Secret Documents

Responsibility for ensuring that Top Secret documents are properly controlled rests with the person originating or acquiring the document. However, ACDA staff did not adhere to document control regulations and procedures. In our sample of 60 of 1,721 safe drawers, we found over 175 uncontrolled Top Secret documents in Washington, D.C., and Geneva.

In Washington, we reviewed the contents of a sample of 34 out of 1,456 safe drawers and found 25 Top Secret documents that had not

been logged into the control system. The ACDA Security Officer is reviewing these findings to determine appropriate administrative or disciplinary action to take.

In 1985, ACDA's Office of Administration reviewed its headquarters records management program, including practices for handling Top Secret material. Its review of safe contents also revealed numerous uncontrolled documents. In its report, the Office concluded that ACDA's procedures were inadequate to control Top Secret information. Its report also noted that ACDA staff had treated Top Secret documents like any other document and had shown no appreciation for the responsibilities attached to possession of Top Secret material. An Information Security Oversight Office inspection conducted shortly after this review identified additional uncontrolled Top Secret documents.

The problem was more pronounced in Geneva, where ACDA officials told us their staff had few, if any, Top Secret documents, and therefore there was no Top Secret control officer or Top Secret document log. In our review of a sample of 26 out of 265 safe drawers we found more than 150 uncontrolled Top Secret documents.

ACDA does not have its own Top Secret control system in Geneva, but ACDA staff have access to the State Department's system. However, according to State Department officials, ACDA had not submitted any Top Secret material for control. According to the State Department's Regional Security Officer, the 150 Top Secret documents we found were placed in the vault for storage. Although regulations require that Top Secret documents be controlled immediately, as of July 1988 they had not yet been logged in.

Required Annual Top Secret Inventories Not Completed

ACDA has not completed the annual inventories of its Top Secret documents, as required by Directive 1, to ensure that all such documents are secure. The 1985 inventory, the most comprehensive since 1979, identified several missing documents, but ACDA did not investigate the losses. Although inventories were started in 1986 and 1987, they were not completed. In May 1988, ACDA began a new inventory effort at headquarters, an effort that was ongoing in July 1988. As of July 1988, ACDA had not taken an inventory of Top Secret documents in Geneva.

According to ACDA's Top Secret control officials, ACDA staff do not always cooperate with inventory efforts. They said that they annually send staff members a list of Top Secret documents assigned to them, asking

that each individual physically inventory assigned holdings and report them. However, employees often ignore the inventory requests.

ACDA Does Not Fully Comply With Standards for Physical Protection

ACDA does not fully comply with regulations regarding the physical protection or marking of classified material either at its Washington headquarters or at its Geneva office. We reviewed the contents of a sample of safe drawers at both locations and found Top Secret, codeword, and other classified information improperly stored. In addition, we found documents marked "NODIS" (No Distribution), which is reserved for communications between the President, the Secretary of State, and the chiefs of mission, stored in unapproved areas.

We determined that ACDA had not changed safe combinations as frequently as required. Also, ACDA had not implemented basic procedures for safeguarding classified information, such as conducting close-of-business-day security checks and posting sign in/out forms for opening and closing safes, and marking document cover sheets with the highest level of classification.

Classified Documents Were Improperly Stored

Executive Order 12356 and Directive 1 stipulate that classified information must be stored in facilities or under conditions designed to prevent unauthorized access. Directive 1 requires that, as a minimum, Top Secret documents be stored in approved safes with three-way combination locks. Secret and Confidential information may be stored in bar lock containers equipped with approved combination padlocks. Codeword information must be stored in an approved vault called a sensitive compartmented information facility. ACDA's regulations require more stringent control overseas, including storing Secret and Confidential information in three-way combination lock safes and storing Top Secret information in a security approved vault. Documents bearing the distribution code NODIS are also to be controlled and stored in the same manner as Top Secret information.

Although most of the documents we reviewed were stored in the proper containers, we found seven Top Secret documents at headquarters improperly stored in a bar lock container and two codeword documents improperly stored in ACDA safes. We reported these violations to ACDA's security officer for investigation. Storage problems were more pronounced in Geneva where we found 152 Top Secret, 99 NODIS, and 68 codeword documents improperly stored outside the vault.

Safe Combinations Not Changed When Required

Directive 1 states that combinations should be changed when (1) an employee knowing the combination terminates employment or is permanently transferred to duties that no longer require the employee's access, (2) when it is known or suspected that an unauthorized person knows the combination, or (3) at least every 12 months. ACDA does not systematically adhere to these criteria for changing the combinations of its safes.

At ACDA headquarters, safe combinations were changed when employees left an office, according to ACDA officials, but there was no systematic method for ensuring the prescribed annual changes. Discussions with ACDA officials and our review showed that some combinations had not been changed for more than 2 years. ACDA security and administrative officials told us that they were unaware of the annual requirement.

In Geneva, combinations to safes were not changed when ACDA personnel using the safes were transferred or their employment was terminated. According to the State Department's Regional Security Officer, the combinations to most safes were last changed during September and October 1987. Although many of the same staff returned for the round of negotiations that began in January 1988, some did not, including one former employee under investigation for unreported trips to the Soviet Union.

ACDA Cannot Account for 62 Safes in Washington, D.C.

Although ACDA does not keep a separate list of its safes, it compiled a list for us in October 1987 based on security container information cards filed in the Office of Security. These cards show the container number, location, combination, and the person(s) having knowledge of the safe combination.

ACDA's Security Office records indicated that ACDA had 331 approved containers that were being used at headquarters to store classified material. After we found inaccuracies in the list, we conducted a physical inventory of all safes in ACDA headquarters offices. Our results differed substantially from ACDA's records. We found only 269 of the containers listed on ACDA's records and an additional 42 for which ACDA had no record. ACDA officials could not explain or account for the 62 safes that could not be located and could not explain why the Security Office did not have information regarding the other 42 safes.

Conducting Close-Of-Business Checks Might Have Reduced Security Violations

Compliance with security regulations to protect national security information entails closing-hour security checks, a process that involves a second person checking the work area at the end of the work day to make sure that any classified materials have been secured appropriately. ACDA regulations state that supervisory officers must designate employees to conduct closing-hour security checks to ensure that all classified material has been properly stored and that containers are locked. An infraction of safeguarding procedures discovered and corrected by an employee designated to conduct such a check is not considered a security violation unless so determined by a higher administrative authority or when it is the final check at a facility not guarded by U.S. citizens. The Information Security Oversight Office has developed standard forms for use in conducting these security checks.

At ACDA headquarters, some offices had formal procedures for close-of-business security checks, but others did not require any checks. There were no second person close-of-business security checks in Geneva.

Our review of ACDA's reported security violations during the last 3 years in Washington and Geneva indicated that the number of violations could be reduced by conducting close-of-business security checks. Most violations involved improper storage of classified material after hours, that is, unlocked safes and classified documents and typewriter ribbons left unsecured. A close-of-business security check system might have minimized the chance of compromise.

Safe Check Regulations Not Implemented

ACDA does not consistently implement regulations requiring certification that containers have been opened, closed, and checked. ACDA regulations require that a security container check sheet be affixed to each safe and that employees indicate the date and time the safe was opened, closed, or checked. Most of the safes in our sample at ACDA headquarters showed use of the required check sheets for opening and closing safes. However, only 45 percent also met the requirements for indication of close-of-business checks. In Geneva, only 24 percent of the safes used by ACDA employees had the security container check sheet, and none of the safes were checked at the end of each work day.

ACDA Does Not Adhere to Marking Requirements for Classified Documents

In reviewing the contents of safe drawers, we examined the classification markings ACDA applied to documents it generated. We found that many ACDA documents did not conform to regulations that require declassification instructions and marking the classification of each paragraph in a document. In addition, cover sheets or transmittal letters were not always marked with the highest classification of material contained in the document to provide ready identification of the document's sensitivity. Further, some documents displayed markings other than those authorized for denoting classification.

The Executive Order and Directive 1 require that documents be marked with declassification instructions, specifying a date, event, or upon determination of the originating agency. Approximately 67 percent of the classified documents we reviewed had declassification instructions. However, most of the documents that had declassification instructions were marked for declassification on the determination of the originating agency, or "Originating Agency's Determination Required (OADR)." The Information Security Oversight Office has criticized ACDA for overuse of OADR on classified documents it generates, citing lack of understanding of appropriate declassification procedures or laxness in applying declassification standards as reasons for relying on OADR as the predominant declassification marking.

Based on its earlier reviews, the Oversight Office also criticized ACDA's lack of adherence to regulations specifying that each paragraph of a document be marked with the highest classification in that paragraph. However, most documents we reviewed contained no such markings.

Although the top page of each document must bear the highest classification of information contained in the document or package being transmitted, we noted that transmittal letters or routing sheets did not always reflect this information. As a result, users could not readily identify the classification of information. For example, during our review of safe contents, we found several unmarked memorandum with classified documents attached.

The Oversight Office also criticized ACDA's use of markings other than Top Secret, Secret, and Confidential—the only markings authorized to denote national security classification. We found a number of documents marked "Secret/Sensitive" and "Top Secret/Sensitive." Several ACDA officials told us that these markings indicated material of political sensitivity that should not be widely disseminated. We asked an ACDA classifying official to review a sample of the "Sensitive" documents. Although

he found most of the documents marked according to the appropriate level of classification, one of the "Secret/Sensitive" documents contained codeword material that should have been appropriately marked and stored in ACDA's vault.

ACDA Has Begun Corrective Actions

ACDA officials have begun taking actions to improve ACDA's information security program. In a May 2, 1988, memorandum to all ACDA staff, the Director of ACDA stated that security is a priority and emphasized the need to protect classified information and material within the agency.

ACDA officials stated that steps are being taken to establish accountability for Top Secret documents. ACDA officials requested that each headquarters bureau and office conduct a thorough review of its files and inventory its Top Secret holdings. According to the Security Officer, ACDA identified an additional 69 uncontrolled Top Secret documents (in addition to the ones we found), and these were added to ACDA's control records. During its inventory, some documents were downgraded or destroyed, and, as of June 30, 1988, ACDA said it had 1,436 accountable documents. According to the Security Officer, ACDA was not able to locate some documents on its Top Secret control log. However, he believes that most documents can be accounted for, and ACDA is continuing efforts to determine their disposition. ACDA is updating its automated records to reflect the information gathered from its headquarters physical inventory.

ACDA is also updating its headquarters records on the number and location of its safes and has asked each of its offices and bureaus to provide current information. ACDA has not devised any specific approach to locate or otherwise explain the missing safes and to assess the potential security risk.

Comments From the Arms Control and Disarmament Agency

UNITED STATES ARMS CONTROL AND DISARMAMENT AGENCY
WASHINGTON

OFFICE OF
THE DIRECTOR

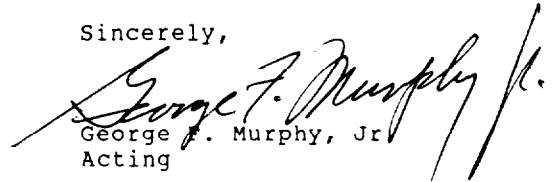
September 27, 1988

Dear Mr. Conahan,

Thank you for your draft report on ARMS CONTROL AND DISARMAMENT AGENCY: Better Controls Needed to Protect Classified Information. We have reviewed your report and wish to commend your staff for a thorough analysis of the ACDA security program. As indicated in the GAO report, your work was conducted from August 1987 to April 1988. Since early 1988 when General Burns took over as the director of this agency, ACDA has instituted a number of changes and improvements in security practices and procedures.

In this connection we are pleased that your report makes reference to these significant corrective actions. Further, we also agree with your five conclusions and recommendations and as indicated, steps have been taken to correct any deficiencies noted by GAO.

Sincerely,



George F. Murphy, Jr.
Acting

Mr. Frank C. Conahan
Assistant Comptroller General
National Security and International Affairs Division
U.S. General Accounting Office
Washington DC 20548

Comments From the Information Security and Oversight Office



Information Security Oversight Office
Washington, DC 20405



September 16, 1988

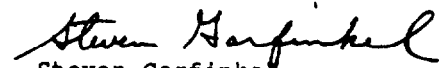
Dear Mr. Conahan:

We appreciate the opportunity to comment on your draft report to the Chairman and Ranking Minority Member of the House Foreign Affairs Committee entitled, "Arms Control and Disarmament Agency: Better Controls Needed to Protect Classified Information." We have reviewed the draft carefully and found it a balanced assessment of the issues that your office evaluated. It shows a good understanding of the classification system in general, and of the Arms Control and Disarmament Agency's (ACDA) program in particular. We also find that, for the most part, the report findings are highly consistent with our observations concerning ACDA's classification program.

We enclose a few suggestions for change. As you will see, these do not involve substantive issues. They are very minor and only indicate a need for clarification and expansion in some areas.

Thank you again for your invitation to comment on the above report. I hope you will find our comments useful. If you have any questions about this letter, please contact Ethel R. Theis at 535-7259.

Sincerely,


Steven Garfinkel
Director

Mr. Frank C. Conahan
Assistant Comptroller
General
U.S. General Accounting Office
Washington, DC 20548

Enclosure

Comments From the Department of State



United States Department of State

Comptroller

Washington, D.C. 20520

September 16, 1988

Dear Mr. Conahan:

I am responding to your letter dated August 30, 1988 to the Secretary which forwarded copies of the draft report entitled "Arms Control and Disarmament Agency: Better Controls Needed to Protect Classified Information" (Code 464126) for review and comment.

The Department has reviewed the report and does not have any comments.

We appreciate having the opportunity to review the draft report.

Sincerely,

A handwritten signature in cursive script that reads "Roger B. Feldman".

Roger B. Feldman

Mr. Frank C. Conahan
Assistant Comptroller General,
National Security and
International Affairs Division,
U.S. General Accounting Office,
Washington, D.C.

Major Contributors to This Report

**National Security and
International Affairs
Division, Washington,
D.C.**

Joseph E. Kelley, Associate Director, (202) 275-4128
Albert H. Huntington, III, Group Director
Mary K. Quinlan, Evaluator-in-Charge
Margaret E. Gaddy, Evaluator

