United States General Accounting Office

GAO

Report to the Chairman, Committee on Rules, House of Representatives

September 1998

EXECUTIVE OFFICE OF THE PRESIDENT

Procedures for Acquiring Access to and Safeguarding Intelligence Information

GAO/NSIAD-98-245

GAO

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

National Security and
International Affairs Division

B-279583

September 30, 1998

The Honorable Gerald B. H. Solomon
Chairman, Committee on Rules
House of Representatives

Dear Mr. Chairman:

This report responds to your request of November 6, 1997, asking us to determine whether the Executive Office of the President (EOP) has established procedures for (1) acquiring personnel access to classified intelligence information, specifically Sensitive Compartmented Information (SCI) and (2) safeguarding such information. You asked that our review include the following offices for which the EOP Security Office provides security support:

- White House Office,
- Office of Policy Development,
- Office of the Vice President,
- National Security Council,
- President's Foreign Intelligence Advisory Board,
- Office of Science and Technology Policy,
- Office of the United States Trade Representative,
- Office of National Drug Control Policy, and
- Office of Administration.

Background

SCI refers to classified information concerning or derived from intelligence sources, methods, or analytical processes requiring exclusive handling within formal access control systems established by the Director of Central Intelligence. The Central Intelligence Agency (CIA) is responsible for adjudicating and granting all EOP requests for SCI access. According to the EOP Security Office, between January 1993 and May 1998, the CIA granted about 840 EOP employees access to SCI.

Executive Order 12958, Classified National Security Information, prescribes a uniform system for classifying, safeguarding, and declassifying national security information and requires agency heads to

- promulgate procedures to ensure that the policies established by the order are properly implemented,
- ensure that classified material is properly safeguarded, and

- establish and maintain a security self-inspection program of their classified activities.

The order also gives the Director, Information Security Oversight Office (an organization under the National Archives and Records Administration), the authority to conduct on-site security inspections of EOP's and other executive branch agencies' classified programs. Office of Management and Budget Circular Number A-123, Management Accountability and Control, emphasizes the importance of having clearly documented and readily available procedures as a means to ensure that programs achieve their intended results.

Director of Central Intelligence Directive 1/14, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, lays out the governmentwide eligibility standards and procedures for access to SCI by all U.S. citizens, including government civilian and military personnel, contractors, and employees of contractors. The directive requires (1) the employing agency to determine that the individual has a need to know;[1] (2) the cognizant Senior Official of the Intelligence Community to review the individual's background investigation and reach a favorable suitability determination; and (3) the individual, once approved by the Senior Official of the Intelligence Community for SCI access, to sign a SCI nondisclosure agreement.[2] Additional guidance concerning SCI eligibility is contained in Executive Order 12968,[3] the U.S. Security Policy Board investigative standards and adjudicative guidelines implementing Executive Order 12968,[4] and Director of Central Intelligence Directive 1/19.

Governmentwide standards and procedures for safeguarding SCI material are contained in Director of Central Intelligence Directive 1/19, Security Policy for Sensitive Compartmented Information and Security Policy Manual.

[1]The "need-to-know" principle is a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function. The prospective recipient shall possess an appropriate security clearance and access approval in accordance with Director of Central Intelligence Directive 1/14.

[2]The SCI nondisclosure agreement establishes explicit obligations on the government and the individual to protect SCI.

[3]Executive Order 12968, Access to Classified Information (Aug. 2, 1995).

[4]U.S. Security Policy Board, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, Investigative Standards for Background Investigations for Access to Classified Information, and Investigative Standards for Temporary Eligibility for Access (Mar. 24, 1997).

The EOP Security Office is part of the Office of Administration. The Director of the Office of Administration reports to the Assistant to the President for Management and Administration. The EOP Security Officer is responsible for formulating and directing the execution of security policy, reviewing and evaluating EOP security programs, and conducting security indoctrinations and debriefings for agencies of the EOP. Additionally, each of the nine EOP offices we reviewed has a security officer who is responsible for that specific office's security program.

As discussed with your office, we reviewed EOP procedures but did not verify whether the procedures were followed in granting SCI access to EOP employees, review EOP physical security practices for safeguarding classified material, conduct classified document control and accountability inspections, or perform other control tests of classified material over which the EOP has custody. (See pp. 8 and 9 for a description of our scope and methodology.)

EOP-Wide Procedures for Acquiring SCI Access Should Be More Specific

The EOP Security Officer told us that, for the period January 1993 until June 1996, (1) he could not find any EOP-wide procedures for acquiring access to SCI for the White House Office, the Office of Policy Development, the Office of the Vice President, the National Security Council, and the President's Foreign Intelligence Advisory Board for which the former White House Security Office[5] provided security support and (2) there were no EOP-wide procedures for acquiring access to SCI for the Office of Science and Technology Policy, the Office of the United States Trade Representative, the Office of National Drug Control Policy, and the Office of Administration for which the EOP Security Office provides security support. He added that there had been no written procedures for acquiring SCI access within the EOP since he became the EOP Security Officer in 1986. In contrast, we noted that two of the nine EOP offices we reviewed issued office-specific procedures that make reference to acquiring access to SCI—the Office of Science and Technology Policy in July 1996 and the Office of the Vice President in February 1997.

According to the EOP Security Officer, draft EOP-wide written procedures for acquiring access to SCI were completed in June 1996 at the time the White House and EOP Security Offices merged. These draft procedures, entitled Security Procedures for the EOP Security Office, were not finalized until March 1998. While the procedures discuss the issuance of EOP

[5]The White House Security Office was abolished on June 19, 1996. On this date, the EOP Security Office assumed responsibility for security support for the EOP offices previously supported by the White House Security Office.

building passes, they do not describe in detail the procedures EOP offices must follow to acquire SCI access; the roles and responsibilities of the EOP Security Office, security staffs of the individual EOP offices, and the CIA and others in the process; or the forms and essential documentation required before the CIA can adjudicate a request for SCI access. Moreover, the procedures do not address the practices that National Security Council security personnel follow to acquire SCI access for their personnel. For example, unlike the process for acquiring SCI access in the other eight EOP offices we reviewed, National Security Council security personnel (rather than the personnel in the EOP Security Office) conduct the employee pre-employment security interview; deal directly with the CIA to request SCI access; and, once the CIA approves an employee for access, conduct the SCI security indoctrination and oversee the individual's signing of the SCI nondisclosure agreement.

Director of Central Intelligence Directives 1/14 and 1/19 require that access to SCI be controlled under the strictest application of the need-to-know principle and in accordance with applicable personnel security standards and procedures. In exceptional cases, the Senior Official of the Intelligence Community or his designee (the CIA in the case of EOP employees) may, when it is in the national interest, authorize an individual access to SCI prior to completion of the individual's security background investigation.

At least since July 1996, according to the National Security Council's security officer, his office has granted temporary SCI access to government employees and individuals from private industry and academia—before completion of the individual's security background investigation and without notifying the CIA. He added, however, that this practice has occurred only on rare occasions to meet urgent needs. He said that this practice was also followed prior to July 1996 but that no records exist documenting the number of instances and the parties the National Security Council may have granted temporary SCI access to prior to this date. CIA officials responsible for adjudicating and granting EOP requests for SCI access told us that the CIA did not know about the National Security Council's practice of granting temporary SCI access until our review.

A senior EOP official told us that from July 1996 through July 1998, the National Security Council security officer granted 35 temporary SCI clearances. This official also added that, after recent consultations with the CIA, the National Security Council decided in August 1998 to refer temporary SCI clearance determinations to the CIA.

EOP Has Not Established Procedures for Safeguarding SCI Material

The EOP-wide security procedures issued in March 1998 do not set forth security practices EOP offices are to follow in safeguarding classified information. In contrast, the Office of Science and Technology Policy and the Office of the Vice President had issued office-specific security procedures that deal with safeguarding SCI material. The Office of Science and Technology Policy procedures, issued in July 1996, were very comprehensive. They require that new employees be thoroughly briefed on their security responsibilities, advise staff on their responsibilities for implementing the security aspects of Executive Order 12958, and provide staff specific guidance on document accountability and other safeguard practices involving classified information. The remaining seven EOP offices that did not have office-specific procedures for safeguarding SCI and other classified information stated that they rely on Director of Central Intelligence Directive 1/19 for direction on such matters.

EOP Has Not Established a Security Self-inspection Program

Executive Order 12958 requires the head of agencies that handle classified information to establish and maintain a security self-inspection program. The order contains guidelines (which agency security personnel may use in conducting such inspections) on reviewing relevant security directives and classified material access and control records and procedures, monitoring agency adherence to established safeguard standards, assessing compliance with controls for access to classified information, verifying whether agency special access programs provide for the conduct of internal oversight, and assessing whether controls to prevent unauthorized access to classified information are effective. Neither the EOP Security Office nor the security staff of the nine EOP offices we reviewed have conducted security self-inspections as described in the order.

EOP officials pointed out that security personnel routinely conduct daily desk, safe, and other security checks to ensure that SCI and other classified information is properly safeguarded. These same officials also emphasized the importance and security value in having within each EOP office experienced security staff responsible for safeguarding classified information. While these EOP security practices are important, the security self-inspection program as described in Executive Order 12958 provides for a review of security procedures and an assessment of security controls beyond EOP daily security practices.

Information Security Oversight Office Has Not Conducted Security Inspections of EOP Activities

Executive Order 12958 gives the Director, Information Security Oversight Office, authority to conduct on-site reviews of each agency's classified programs. The Director of the Information Security Oversight Office said his office has never conducted an on-site security inspection of EOP classified programs. He cited a lack of sufficient personnel as the reason for not doing so and added that primary responsibility for oversight should rest internally with the EOP and other government agencies having custody of classified material.

The Director's concern with having adequate inspection staff and his view on the primacy of internal oversight do not diminish the need for an objective and systematic examination of EOP classified programs by an independent party. An independent assessment of EOP security practices by the Information Security Oversight Office could have brought to light the security concerns raised in this report.

Recommendations

To improve EOP security practices, we recommend that the Assistant to the President for Management and Administration direct the EOP Security Officer to

- revise the March 1998 Security Procedures for the EOP Security Office to include comprehensive guidance on the procedures EOP offices must follow in (1) acquiring SCI access for its employees and (2) safeguarding SCI material and
- establish and maintain a self-inspection program of EOP classified programs, including SCI in accordance with provisions in Executive Order 12958.

We recommend further that, to properly provide for external oversight, the Director, Information Security Oversight Office, develop and implement a plan for conducting periodic on-site security inspections of EOP classified programs.

Agency Comments and Our Evaluation

We provided the EOP, the Information Security Oversight Office, and the CIA a copy of the draft report for their review and comment. The EOP and the Information Security Oversight Office provided written comments, which are reprinted in their entirety as appendixes I and II, respectively. The CIA did not provide comments.

In responding for the EOP, the Assistant to the President for Management and Administration stated that our report creates a false impression that the security procedures the EOP employs are lax and inconsistent with established standards. This official added that the procedures for regulating personnel access to classified information are Executive Order 12968 and applicable Security Policy Board guidelines and Executive Order 12968 and Executive Order 12958 for safeguarding such information. The Assistant to the President also stated that the report suggests that the EOP operated in a vacuum because the EOP written security procedures implementing Executive Order 12968 were not issued until March 1998. The official noted that EOP carefully followed the President's executive orders, Security Policy Board guidelines and applicable Director of Central Intelligence Directives during this time period. While the EOP disagreed with the basis for our recommendation, the Assistant to the President stated that EOP plans to supplement its security procedures with additional guidance.

We agree that the executive orders, Security Policy Board guidelines, and applicable Director of Central Intelligence Directives clearly lay out governmentwide standards and procedures for access to and safeguarding of SCI. However, they are not a substitute for local operating procedures that provide agency personnel guidance on how to implement the governmentwide procedures. We believe that EOP's plan to issue supplemental guidance could strengthen existing procedures.

The Assistant to the President also stated that it is not accurate to say that the EOP has not conducted security self-inspections. This official stated that our draft report acknowledges that "security personnel conduct daily desk, safe, and other security checks to ensure that SCI and other classified material is properly safeguarded." The Assistant to the President is correct to point out the importance of daily physical security checks as an effective means to help ensure that classified material is properly safeguarded. However, such self-inspection practices are not meant to substitute for a security self-inspection program as described in Executive Order 12958. Self-inspections as discussed in the order are much broader in scope than routine daily safe checks. The order's guidelines discuss reviewing relevant security directives and classified material access and control records and procedures, monitoring agency adherence to established safeguard standards, assessing compliance with controls for access to classified information, verifying whether agency special access programs (such as SCI) provide for the conduct of internal oversight, and assessing whether controls to prevent unauthorized access to classified

information are effective. Our report recommends that the EOP establish a self-inspection program.

In commenting on our recommendation, the Assistant to the President said that to enhance EOP security practices, the skilled assistance of the EOP Security Office staff are being made available to all EOP organizations to coordinate and assist where appropriate in agency efforts to enhance self-inspection. We believe EOP security practices would be enhanced if this action were part of a security self-inspection program as described in Executive Order 12958.

The Director, Information Security Oversight Office noted that our report addresses important elements of the SCI program in place within the EOP and provides helpful insights for the security community as a whole. The Director believes that we overemphasize the need to create EOP specific procedures for handling SCI programs. He observed that the Director of Central Intelligence has issued governmentwide procedures on these matters and that for the EOP to prepare local procedures would result in unnecessary additional rules and expenditure of resources and could result in local procedures contrary to Director of Central Intelligence Directives. As we discussed above, we agree that the executive orders, Security Policy Board guidelines, and applicable Director of Central Intelligence Directives clearly lay out governmentwide standards and procedures for access to and safeguarding of SCI. However, they are not a substitute for local operating procedures that provide agency personnel guidance on how to implement the governmentwide procedures.

The Director agreed that his office needs to conduct on-site security inspections and hopes to begin the inspections during fiscal year 1999. The Director also noted that the primary focus of the inspections would be classification management and not inspections of the SCI program.

Scope and Methodology

To identify EOP procedures for acquiring access to SCI and safeguarding such information, we met with EOP officials responsible for security program management and discussed their programs. We obtained and reviewed pertinent documents concerning EOP procedures for acquiring SCI access and safeguarding such information.

In addition, we obtained and reviewed various executive orders, Director of Central Intelligence Directives, and other documents pertaining to acquiring access to and safeguarding SCI material. We also discussed U.S.

government security policies pertinent to our review with officials of the Information Security Oversight Office and the U.S. Security Policy Board. Additionally, we met with officials of the CIA responsible for adjudicating and granting EOP employees SCI access and discussed the CIA procedures for determining whether an individual meets Director of Central Intelligence Directive eligibility standards.

As discussed with your office, we did not verify whether proper procedures were followed in granting SCI access to the approximately 840 EOP employees identified by the EOP Security Officer. Also, we did not review EOP physical security practices for safeguarding SCI and other classified material, conduct classified document control and accountability inspections, or perform other control tests of SCI material over which the EOP has custody.

We performed our review from January 1998 until August 1998 in accordance with generally accepted government auditing standards.

At your request, we plan no further distribution of this report until 30 days after its issue date. At that time, we will provide copies to appropriate congressional committees; the Chief of Staff to the President; the Assistant to the President for Management and Administration; the Director, Information Security Oversight Office; the Director of Central Intelligence; Central Intelligence Agency; the U.S. Security Policy Board; the Director of the Office of Management and Budget; and other interested parties.

Please contact me at (202) 512-3504 if you or your staff have any questions concerning this report. Major contributors to this report were Gary K. Weeter, Assistant Director and Tim F. Stone, Evaluator-in-Charge.

Sincerely yours,

Richard Davis
Director, National Security
Analysis

Contents

Abbreviations

CIA	Central Intelligence Agency
EOP	Executive Office of the President
SCI	Sensitive Compartmented Information

Comments From the Assistant to the President for Management and Administration

Note: GAO comment supplementing those in the report text appears at the end of this appendix.

THE WHITE HOUSE

WASHINGTON

September 23, 1998

Mr. Richard Davis
Director, National Security Analysis
National Security and
International Affairs Division
Room 4015
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Davis:

We are writing in response to your September 11, 1998 letter and draft report for the Executive Office of the President (EOP), Procedures for Acquiring Access to and Safeguarding Intelligence Information. Unfortunately, the GAO report creates the false impression that the security procedures employed at the EOP are lax and inconsistent with established standards. Nothing could be further from the truth. In fact, as the evidence provided to the GAO makes abundantly clear, EOP security officials are experienced professionals who have executed their responsibilities diligently and with great attention to detail.

The GAO report also implies that these experienced professionals have not fulfilled their obligations under the law. This is completely unsupported by any reading of the facts. The extensive information provided by the EOP to the GAO auditors plainly demonstrates that the EOP has conscientiously abided by security precautions.

The EOP has made available to the GAO audit team reviewing EOP security procedures key personnel and relevant documents. In fact, the General Counsel of the Office of Administration and the EOP Security Office Chief have personally devoted a substantial number of hours to facilitate the GAO's audit. Numerous other EOP officials have also devoted significant amounts of time to assist the GAO auditors.

After the submission of hundreds of pages of documentation, more than ten meetings with the GAO auditors and more than ten individual interviews with EOP entities, the report still contains errors and statements that generate mis-impressions. It is our hope that the GAO will make the appropriate corrections to the report prior to its submission to the Congress.

See comment 1.

In short, the EOP has established procedures for regulating personnel access to classified information; also, the EOP has a rigorous program, administered by career professional security officers, to safeguard classified information. The procedures in question are contained in E.O. 12968 and applicable Security Policy Board (SPB) guidelines. The safeguards in question are also contained E.O. 12968 and in E.O. 12958.

The report suggests that the EOP, and its constituent entities, operated in a vacuum because the EOP written security procedures implementing E.O. 12968 were not issued until March 1998. In fact, the EOP carefully followed the authoritative guidance set forth in the President's Executive Orders, SPB guidelines, and applicable Director of Central Intelligence Directives (DCI/Ds) throughout this time period. The President's Executive Orders are the cornerstones of the EOP's security programs and provide the basis for the adjudication of access to classified information, with or without subsequent guidelines. The EOP has found that the Executive Orders and SPB guidelines provide clear guidance that has been implemented with care in order to safeguard classified information and regulate access to it.

With respect to the draft report's comments relating to temporary SCI clearances, during the period July 1996 through July 1998, the NSC Security Officer, a professional career security officer on detail, granted 35 temporary SCI clearances subject to issuance by the CIA of a final SCI clearance. Before considering issuance of a temporary SCI clearance, the Security Officer conducted a thorough review of available background information from the completed SF-86, obtained the results of the FBI name check, and received a progress report from the FBI when the background check was substantially completed. Only if this careful examination revealed no derogatory information would a temporary clearance be granted. Although this process has been implemented successfully with no adverse indications, the NSC decided in August 1998, after consultations with CIA Headquarters personnel and with a view towards simplifying this process, to refer temporary SCI clearance determinations to CIA Headquarters.

The headline for the section of the draft report on self-inspections -- EOP HAS NOT CONDUCTED SECURITY SELF-INSPECTIONS -- is simply not accurate. Indeed, the draft report acknowledges that "security personnel conduct daily desk, safe, and other security checks to ensure that SCI and other classified material is properly safeguarded." The EOP operates consistently with the self-inspection guidelines issued by the Information Security Oversight Office pursuant to E.O. 12958 for safeguarding classified information, which is the primary focus of this draft report.

The GAO report includes three recommendations. One of the three recommendations included in the GAO report is that the EOP "initiate a self inspection program." As we have stated and supported on numerous occasions to the GAO auditors, our current self-inspection practices are effective. Nevertheless, we are continuing our efforts to enhance EOP security practices. We have made available to all EOP organizations the skilled assistance of our EOP security office staff to coordinate and assist where appropriate in agency efforts to enhance self-inspection.

The GAO also recommends that we revise the Security Procedures for the EOP Security Office to include "comprehensive guidance" on "acquiring SCI access" and "properly safeguarding SCI material." In fact, the EOP Security Procedures do include comprehensive guidance. As we pointed out to the GAO auditors on several occasions, paragraph 10(c)of the Security Procedures incorporates by reference guidance for obtaining SCI access. Although we disagree with the basis for the GAO recommendation, we have initiated an effort to supplement the Security Procedures with additional guidance.

Finally, the draft report recommends that the Information Security Oversight Office conduct periodic on-site reviews of the EOP security process. We stand ready to work with the ISOO in any such undertaking.

We would like to request a meeting with the GAO auditors to discuss the issues raised in this letter in addition to other technical corrections to the GAO report. If there is anything that I or any member of my staff, can do to be of assistance, please feel free to contact Mark Lindsay (202) 456-3880.

Sincerely yours,

Virginia M. Apuzzo
Assistant to the President for
Management and Administration

The following is GAO's comment to the Assistant to the President for Management and Administration's letter dated September 23, 1998.

GAO Comment

1. A representative of the Executive Office of the President (EOP) told us that the errors referred, for example, to statements in ours draft report that the EOP does not conduct self-inspections and that the EOP lacks written procedures.

Comments From the Information Security Oversight Office

Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW *Washington, DC 20408*

September 18, 1998

Mr. Richard Davis
Director, National Security Analysis
National Security and International Affairs Division
United States General Accounting Office
Washington, DC 20548

Dear Mr. Davis:

Subject: **Comments on General Accounting Office (GAO) Report "Executive Office of the President: Procedures for Acquiring Access to and Safeguarding Intelligence Information"**

Thank you for the opportunity to comment on the subject draft GAO report. It addresses important elements of the Sensitive Compartmented Information (SCI) program in place within the Executive Office of the President (EOP) and provides helpful insights for the security community as a whole. The conclusions drawn in three areas of the report prompt the Information Security Oversight Office (ISOO) to offer the following comments.

(1) ISOO believes the draft report overemphasizes the issuance of individual office and agency procedures for handling SCI. While Executive Order 12958 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, the Director of Central Intelligence (DCI) prescribes the augmentation of those procedures for SCI, both under the Executive order and the DCI's statutory authorities. As noted in the report, the DCI has issued Government-wide standards and procedures for access to SCI and for safeguarding SCI with Director of Central Intelligence Directives (DCIDs) 1/14 and 1/19, respectively.

Most executive branch agencies rely upon the DCIDs exclusively as their security procedures documents for SCI, rather than generating others. Requiring agencies to generate additional procedures documents for SCI would result in unnecessary additional rules and expenditure of resources, and could result in procedures contrary to the DCIDs, particularly, if the DCI does not review and approve them. Ensuring that EOP offices and executive branch agencies have ready access to the DCIDs could alleviate concerns about the need for detailed procedures in each office and agency.

(2) Several factors have prevented ISOO from conducting compliance inspections for the past several years. These include the drafting and implementing of E.O. 12958, with its increased functions for ISOO. At the same time, the size of ISOO's staff has decreased by one-third to the point where its total professional and clerical staff numbers 10 people. Nevertheless, we agree that ISOO needs to be conducting inspections and we hope to do so during fiscal year 1999.

Your report suggests, however, that ISOO's inspections would cover SCI as it relates both to the issuance of SCI clearances and the safeguarding of SCI information. These areas would never be the primary or even secondary focus of ISOO's compliance inspections. First, ISOO does not have any jurisdiction over the personnel security (clearance) system. Second, ISOO's primary concern in classification management would not ordinarily focus on the SCI program. In other words, external oversight of the EOP's SCI programs would only coincidentally result from increased ISOO inspections.

(3) Finally, your report raises concerns about the granting of interim clearances for SCI access at the National Security Council (NSC). While we share the report's concerns about the possibility for abuse in this area, we also recognize and understand the NSC's responsibilities to the President. With respect to information generated by the Intelligence Community, having appropriately cleared individuals on the job in a timely manner is essential. Because the SCI program is so large and widely dispersed across the government, ISOO understands the NSC's need to have the ability to grant interim clearances, under specific conditions, so that individuals can perform their duties. Properly managing and controlling how these interim clearances are granted would be an important element of oversight. Your report suggests that the DCI is addressing this issue with the NSC.

Please call me on 202-219-5250 if you have any questions concerning our comments on your draft report. Again, we appreciate the opportunity to comment.

Sincerely,

Steven Garfinkel

Steven Garfinkel
Director

Ordering Information

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

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

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

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested