GPO

Report on the Management Control Program within the Office of Information Resources Management (OIRM)

September 1999 99-09

Office of Audits

UNITED STATES GOVERNMENT PRINTING OFFICE
OFFICE OF THE INSPECTOR GENERAL

memorandum

DATE: September 29, 1999

REPLY TO
ATTN OF: Inspector General

SUBJECT: Report on the Management Control Program within the Office of Information Resources Management (OIRM)

TO: Public Printer
Director, Office of Information Resources Management
Director, Office of Administrative Support

An Office of Inspector General audit team conducted an audit to assess the adequacy and effectiveness of OIRM's management control program from May 1997 through February 1999. The audit noted that as of February 1999, OIRM had identified and completed self-assessments of six major areas involving 81 controls. While OIRM attempted to identify, assess, and test its internal controls, the work was incomplete. Of the 42 high level controls identified by us in our application of a leading comprehensive methodology, relatively few were addressed by OIRM.

The audit recommends that the Director, OIRM, with assistance from the Director, Administrative Support Division, implement 17 recommendations to strengthen the internal controls over: (1) completing accurate self-assessments with documentation; (2) implementing and resolving open audit recommendations; (3) testing software program changes; (4) authorizing access to the computer system; (5) developing and maintaining collective and individual training plans; and (6) keeping only used systems software in the mainframe.

The Director, OIRM, and the Director, Office of Administrative Support, agreed with the majority of findings and recommendations, and have begun implementing 14 of the 17 recommendations. The Director, OIRM, disagreed with the three recommendations on adopting a comprehensive control framework to complete accurate self-assessments of OIRM's internal controls. (See Appendix III.)

We note, however, that in agreeing with the third and fourth findings and their accompanying recommendations, the Director, OIRM, made her agreement contingent upon receiving additional funding and staffing. Such contingent agreement is tantamount to disagreement, since most managers could accomplish virtually any objective with sufficient funding and staffing. OIRM's comments demonstrate the low priority given to internal controls within that organization. This low priority was further illustrated by the Director's recent response to an OIG request that she furnishes us with the results of any internal control reviews conducted by OIRM during Fiscal Year 1999. The Director, OIRM, responded that no internal control reviews were performed this year due to Y2K remediation. (See Appendix VI.)

Mr. Kevin Kaporch, Supervisory Computer Specialist, and Mr. Brian Buxton, Auditor-In-Charge, conducted the audit.

I appreciate the cooperation and courtesies extended during the audit by the officials and staff of OIRM, the Office of Administrative Support, and the Office of Personnel.

Robert G. Andary
ROBERT G. ANDARY

Report on the Management Control Program Within the Office of Information Resources Management (OIRM)

TABLE OF CONTENTS

U.S. Government Printing Office
Office of the Inspector General
Office of Audits

Report on the Management Control Program Within the Office of Information Resources Management (OIRM)

RESULTS IN BRIEF

As of February 1999, OIRM had identified and completed self-assessments of six major areas involving 81 controls. Those six major areas were: Organization and Management of OIRM, Application Systems Development, Application Systems Maintenance, Systems Software Support, Computer Operations, and Data Entry Controls.

The results of our review indicated that the internal control self-assessments performed appeared to be accurate, but with major exceptions as noted below. While OIRM attempted to identify, assess, and test its internal controls, the work was incomplete. Of the 42 high level controls identified by us in our application of a leading comprehensive methodology, relatively few were addressed by OIRM. (See Finding 1 and Appendix I.)

Controls that were not self-assessed included 33 high level controls within four domains as follows:

- Planning and Organization;
- Acquisition and Implementation;
- Delivery and Support; and
- Monitoring.

Other unassessed controls included nine high level controls concerning the following:

- Networks; and
- Electronic Data Interchange.

Additionally, OIRM did not adequately test and document its internal controls before it prepared its self-assessments. (See Findings 1 and 2.) This is the primary cause for the inaccuracies discovered in this review. Furthermore, we noted areas where controls could be strengthened to improve the operating effectiveness and efficiency of OIRM. (See Findings 3 through 8.)

The findings in our report cannot be corrected without the commitment of executive management and the proper staffing of OIRM. In many instances, we identified a lack of adequate management attention and inadequate staffing as the primary causes behind OIRM's inability to correct long-standing audit deficiencies and fully implement the Government Printing Office (GPO) internal control program. Additional management emphasis is needed in light of the challenges OIRM has in providing a year 2000 (Y2K) compliant environment for GPO. Successful implementation of a Y2K program is predicated upon strong internal controls. Implementing our recommendations will strengthen internal controls in OIRM.

Our audit also assessed OIRM's susceptibility to fraud, waste, and abuse. While we noted no instances of fraud or abuse, we did find that unused and outdated software was still resident on the mainframe. This can adversely impact on capacity planning and management. Since we reviewed only a small portion of the activities and controls in OIRM, we were unable to provide a complete assessment as to which areas are most at risk.

RECOMMENDATIONS

OIRM should adopt a comprehensive methodology to govern assessment of its internal controls, such as the one used by the OIG in this assessment: "CobiT: Control Objectives for Information and Related Technology." See Findings 1 and 2. OIRM should also test, document, and properly report these results (See Finding 3) and include in these tests the additional controls described in Finding 1 and Appendix I.

CobiT is accepted by external auditors, such as KPMG Peat Marwick LLP, and has been referenced by the General Accounting Office (GAO) in its *Federal Information System Controls Audit Manual* (FISCAM), which is required to be followed by the external auditors of GPO's financial statements. By implementing a controls framework and methodology such as CobiT, OIRM can substantially improve its information systems controls as well as its control self-assessment process.

Additionally, for OIRM to reduce its management control risks, it should:

- Reassess its internal controls and conduct and document appropriate tests to ensure the controls are functioning effectively.

Improve documentation by:

- Testing internal controls and retaining documentation;

- Documenting all systems development and maintenance activities and include this in the automated tracking system;
- Updating policies and procedures manuals;
- Ensuring all document-approved changes to systems software have written approval to implement them; and
- Requesting a staffing analysis, updating position descriptions, and creating new position descriptions -- when warranted.

Improve outstanding audit recommendations by:

- Implementing or resolving all outstanding audit recommendations.

Improve application software change control procedures by:

- Ensuring that all software changes are properly tested in the test region.

Improve access controls by:

- Reconfirming security procedures with the Office of Personnel, Comptroller, and the Office of Administrative Support to preclude personnel whose clearance or employment status has changed from inappropriately accessing OIRM managed systems; and
- Periodically validating access lists of personnel authorized to receive application system reports generated by the data center.

Improve training by:

- Developing collective and individual training plans with a training budget; and
- Considering the appointment of a training coordinator and ensuring that all computer-related training, regardless of funding source, augment OIRM's training records.

Improve software usage by:

- Removing outdated and unused software still resident on the mainframe and changing the status of unused software applications from "operational" to "retired" in the systems level documentation.

BACKGROUND

The Office of Information Resources Management (OIRM), under the supervision of the Director, provides information resources management services to GPO, other Federal agencies, and private individuals. OIRM performs feasibility studies to determine the need for GPO-wide information systems and programs. OIRM also designs, develops, and maintains agency data processing, office automation, local and wide area networks, and telecommunications systems. OIRM is divided into: (1) the Information Services Division, which contains the Office Automation Services Group and the Data Processing Services Group and (2) the Information Systems Development Division, which contains the Database Design and Information Management Group and the Systems Development Group.

On May 28, 1997, the Public Printer issued GPO Instruction 825.18A, *Internal Control Program*. Its purpose was to prescribe policies and standards and assign responsibilities for conducting vulnerability assessments and internal control reviews of programs and activities of the GPO. The instruction borrowed heavily from the Federal Managers Financial Integrity Act (FMFIA) of 1982, which mandated that Executive Branch Agencies improve their internal controls by requiring internal control self-assessments and annual reports thereon to the Office of Management and Budget (OMB). GPO is not subject to FMFIA.

Fiscal Year	Significant Events
1995	The Public Printer requires department heads to implement an internal control program within their organization. OIRM documents their internal control program with the publication of the "OIRM Management Control Review Guide."
1996-1997	OIRM identifies and self-assesses 81 controls.
1997	The Public Printer issues GPO Instruction 825.18A, *Internal Control Program,* and the OIG initiates an audit of OIRM's management control program.
1999	The OIG completes its review of OIRM's management control program and OIRM agrees to consider adopting the framework delineated in CobiT in response to a recommendation made by KPMG Peat Marwick LLP in their audit of the 1997 financial statements of GPO.

GPO Instruction 825.18A, *Internal Control Program,* describes internal controls as:

> "The organization, policies, and procedures used to reasonably ensure that:
>
> (1) programs achieve their intended results;
> (2) resources are used consistent with agency mission;
> (3) programs and resources are protected from waste, fraud, and mismanagement;
> (4) laws and regulations are followed; and
> (5) reliable and timely information is obtained, maintained, reported, and used for decisionmaking."

Management control is also defined by the American Institute of Certified Public Accountants (AICPA) in the "Report of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control - Integrated Framework,"* as follows:

> "The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."

A good source for descriptions of information technology (IT) control objectives can be found in CobiT: "Control Objectives for Information and Related Technology," published by the Information Systems Audit and Control Foundation. Their definition of IT control is:

> "A statement of the desired results or purpose to be achieved by implementing control procedures in a particular IT activity."

The above are important to GPO because these control definitions establish a framework in which this agency will most likely be evaluated in future audits conducted by the General Accounting Office (GAO), other external auditors, and the OIG. COSO will soon be incorporated into GAO's *Standards for Internal Controls in the Federal Government*. CobiT represents a framework of information system (IS) controls that GPO has been evaluated on in this audit as well as the 1997 financial statement audit conducted by KPMG Peat Marwick LLP. CobiT is recognized by the GAO as an authoritative source for IS control criteria.

GPO Instruction 825.18A requires that a report on management controls in the form of a statement of assurance from GPO managers be provided to the Public Printer annually. The results of our audit can assist the Director, OIRM, in providing such an assurance statement. The audit can also serve to identify to the Public Printer the risks, exposures, and issues pertaining to information technology that will continue to be addressed by third party elements such as the GAO and the external auditors of GPO's financial statements.

In 1995 the Director, OIRM, initiated an internal control program in response to a task from the Public Printer for all department heads to establish management controls for their organizations and conduct internal control reviews on them. The Director's program included areas to be evaluated and the control objectives and techniques for each, as well as a schedule for internal control self-assessments together with the prescribed format. The program was documented with the internal publication of the "OIRM Management Control Review Guide" in September 1995.

OIRM management had already prepared internal control assessments using the "OIRM Management Control Review Guide," dated September 1995. The six major areas assessed were: (1) Organization and Management of OIRM, (2) Application Systems Development, (3) Application Systems Maintenance, (4) Systems Software Support, (5) Computer Operations, and (6) Data Entry Controls. As of May 1997, OIRM had identified and self-assessed these six major areas involving 81 controls. However, no vulnerability assessments were performed; nor were any material internal control weaknesses identified. As of September 1998, OIRM management planned to conduct reviews of its organization and management, as well as its computer operations.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objective of this audit was to assess the adequacy and effectiveness of OIRM's management control program. To this end, three sub-objectives were established, as follows:

- Evaluate the adequacy of internal control assessments conducted by OIRM personnel;

- Assess the adequacy of follow up actions to correct OIRM related deficiencies identified by external auditors and the OIG in prior audit reports; and

- Identify areas within OIRM susceptible to fraud, waste, and abuse.

The audit was conducted from the period of May 1997 through February 1999 and was performed in accordance with generally accepted Government auditing standards (GAGAS) issued by the Comptroller General of the United States, as well as standards promulgated by the Information Systems Audit and Control Association (ISACA).

The methodology used consisted of interviews, on-line queries, observations, examinations of documents, and reperformance (testing) to assess the validity of reported internal control self-assessments and corrective action taken on outstanding audit recommendations.

The control framework and standards established by the Information Systems Audit and Control Foundation (ISACF) in CobiT was used as one criteria to assess OIRM's controls, because OIRM has not adopted a similar framework to guide its internal control revisions. CobiT is recognized as one of the most comprehensive and up-to-date sets of information system control standards in business and government. We also used applicable standards contained in "Control Objectives, Controls in an Information Systems Environment: Objectives, Guidelines and Audit Procedures," published by ISACF.

CobiT is designed to be used by three distinct audiences: (1) management, to help them balance risk and control investment in an often unpredictable IT environment, (2) users, to obtain assurance on the security and controls of IT services provided by internal or third parties, and (3) auditors, to substantiate their opinions on internal controls and to provide management advice on control-related matters.

The control objectives delineated in CobiT are referenced in GAO's *Federal Information System Controls Audit Manual* (FISCAM), dated January 1999 and are required to be used by the external auditors of GPO's financial statements.

Because many of the information systems controls the OIG assessed are evaluated as part of the financial statement audits of GPO, we used control standards outlined in the report of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), published in 1992 and adopted by the American Institute of Certified Public Accountants (AICPA) in Statement on Auditing Standards (SAS) Number 78, "Consideration of Internal Control in a Financial Statement Audit." COSO is also referenced in the FISCAM, as well as GAO's *Financial Audit Manual* (FAM), which the external auditors are also required to use in their financial statement audits of GPO. In addition, we used internal control standards contained in AICPA SAS Number 60 "Communication of Internal Control Structure Related Matters Noted in an Audit," and incorporated in GAGAS for financial statement audits that the external auditors of GPO's financial statements are required to follow.

We reviewed:

- Arthur Andersen, LLP's prepared "Comments and Suggestions for Consideration," dated January 1996, which was performed as part of the 1995 financial statement audit;

- KPMG Peat Marwick LLP's "Management Letter" to GPO dated as of September 30, 1997, to determine if appropriate corrective action had been taken for each pertinent reportable condition and management letter comment;

- IT related findings contained in the "Management Audit of the Government Printing Office," dated May 21, 1998, and conducted by Booz-Allen & Hamilton; and

- Prior OIG reports pertaining to OIRM to determine which findings and recommendations were still outstanding and evaluated the corrective action taken.

Based on the results of work performed, the OIG assessed the susceptibility of OIRM to fraud, waste, and abuse. Because we reviewed only a small portion of the activities and controls in OIRM, we were unable to provide a complete assessment as to which areas are most at risk.

PRIOR AUDIT COVERAGE

The OIG, Arthur Andersen, LLP, KPMG Peat Marwick LLP, and Booz-Allen & Hamilton have conducted previous audits of GPO and OIRM in which there are still outstanding audit recommendations. In addition, GAO initiated a review of GPO's Year 2000 readiness in November 1997, as requested by Congress. This continuing oversight by GAO, which materially affects OIRM, has, as of yet, produced no published findings and recommendations. Finding 4 of this report summarizes prior uncorrected recommendations pertaining to OIRM.

FINDINGS AND RECOMMENDATIONS

1. COMPLETENESS OF INTERNAL CONTROL SELF-ASSESSMENTS (REVIEWS)

FINDING

OIRM's internal control self-assessment program is incomplete because OIRM lacked an integrated framework of generally accepted information technology control objectives for guidance in implementing its internal control program.

OIRM did not completely identify and self-assess its control objectives, because it lacked such a framework. OIRM lacked an up-to-date, detailed definition and explanation of applicable internal control objectives and techniques, as well as detailed guidance and support for assessing them. They also lacked the human resources and time to properly identify and evaluate all of the information systems controls for which OIRM should be responsible.

For many organizations today, information and the technology that supports it are an organization's most valuable asset. GPO is not an exception and bases its success on an effective management of information and related technology. While GPO is increasingly dependent on information systems in which it has made substantial investments, it is also increasingly vulnerable to both external and internal threats to the security and control of these systems and the information it produces.

The following 42 high level controls, organized into six major areas as delineated by the Information Systems Audit and Control Foundation (ISACF), were neither identified by nor completely self-assessed by OIRM. OIRM relied on control objectives derived from Executive Branch sources. The 42 high level controls are as follows:

I. <u>Planning and Organization</u>

1. Define a Strategic Information Technology (IT) Plan
2. Define the Information Architecture
3. Determine the Technology Direction
4. Define the IT Organization and Relationships
5. Manage the Investment in Information Technology
6. Communicate Management Aims and Direction
7. Manage Human Resources

8. Ensure Compliance with External Requirements
9. Assess Risks
10. Manage Projects
11. Manage Quality

II. <u>Acquisition and Implementation</u>

12. Identify Solutions
13. Acquire and Maintain Application Software
14. Acquire and Maintain Technology Architecture
15. Develop and Maintain IT Procedures
16. Install and Accredit Systems
17. Manage Changes

III. <u>Delivery and Support</u>

18. Define Service Levels
19. Manage Third Party Services
20. Manage Performance and Capacity
21. Ensure Continuous Service
22. Ensure Systems Security
23. Identify and Attribute Costs
24. Educate and Train Users
25. Assist and Advise IT Customers:
26. Manage the Configuration
27. Manage Problems and Incidents
28. Manage Data
29. Manage Facilities
30. Manage Operations

IV. <u>Monitoring</u>

31. Monitor the Process
32. Assess Internal Control Adequacy
33. Obtain Independent Assurance

V. <u>Networks</u> (as they now apply to OIRM)

34. Network Management Controls
35. Network Data Controls
36. Network Software Controls

37. Network Operations Controls
38. Network Data Security Controls
39. LAN Management Controls
40. LAN Security Controls

VI. Electronic Data Interchange (EDI)

41. EDI Management Controls
42. EDI Operations Controls

The high level controls listed above are derived from CobiT. OIRM has not yet adopted a comparable framework and set of standards. Specific control objectives pertaining to these high level controls are contained in Appendix I of this report.

GPO Instruction 825.18A describes the policy, responsibilities and standards for the internal control program and states, "GPO shall maintain effective systems of accounting and management control." As well, "Department, Service, Staff, and Office Heads are responsible for the development and maintenance of internal controls within their respective programs, functions, and activities, to prevent or deter the loss or abuse of public assets."

The use of CobiT, or a similar comprehensive framework, can assist OIRM, as well as GPO in further developing and maintaining an effective system of control over information and its related technology.

The effect of not completely identifying and self-assessing internal controls could provide the Public Printer and other concerned parties (GPO management, GPO OIG, Congress, the General Accounting Office, external auditors of the financial statements, and the public) with a possibly inaccurate perception of the effectiveness of internal controls within OIRM.

RECOMMENDATIONS

The Director, OIRM, should:

- Adopt a comprehensive control framework for conducting internal control assessments of information technology such as is delineated in the second edition of "CobiT: Control Objectives For Information Technology and Related Technology," or a similar generally accepted framework (9909-01); and

- Update the "OIRM Management Control Review Guide" and perform internal control assessments of the information systems controls delineated herein that have not yet been evaluated (9909-02).

MANAGEMENT COMMENTS

The Director, OIRM, disagreed with the finding and recommendations as stated in Appendix III of this report. In part, the Director stated,

> "For the most part, OIRM believes our control framework is adequate. Many of the six major areas and resultant 42 high-level controls either are assigned to other GPO organizations, or are not appropriate at GPO."
>
> "OIRM cannot adopt a comprehensive control framework to the level of detail and specificity required by '*Cobit*' with its present staffing levels. The GPO should not follow '*Cobit*' which was not designed for the Federal Government, is not used by other Federal Agencies, and is not mandatory."

In conclusion, the Director stated,

> "Predicated on the above, OIRM cannot implement the first part of the recommendation, and disagrees with the second part."

INSPECTOR GENERAL'S RESPONSE

OIRM management took exception to various criteria used by the OIG including CobiT. Further, OIRM believes that guidance from the *"Arthur Anderson Guide for Studying and Evaluating Internal Controls in the Federal Government...the Federal Managers Financial Integrity Act of 1982, and OMB Circular A-123..."* is more appropriate. While CobiT is not specifically applicable to the GPO neither are those criteria listed by OIRM which have become dated and lack the specificity to assist in developing controls in a contemporary Information Technology environment.

We agree that the CobiT framework is large and likely exceeds OIRM's span of control. However, we are suggesting that OIRM use what is applicable from that methodology to ensure that they have adequately addressed their control environment to the level of detail they deem appropriate. As evidenced by the results of this report, reliance on their preferred guidance/criteria has not served OIRM well.

2. ACCURACY OF INTERNAL CONTROL SELF-ASSESSMENTS (REVIEWS)

FINDING

OIRM management identified and self-assessed 81 control objectives. The OIG evaluated 61 of these self-assessments. Of the remaining 20 self-assessments, three were not tested by the OIG, because it would have been impractical and inefficient. Limited time and generally worded control objectives precluded the efficient and effective testing of these three controls. Preliminary analysis of the remaining 17 self-assessments, in the area of systems development, indicated that controls were likely to be ineffective. Therefore, further testing was not warranted.

With the following exceptions, we confirmed management statements that controls were in place and operating. Of the 61 control objectives tested, management's assertions pertaining to 16 objectives could not be fully supported, and the corresponding risk ratings appeared to be lower than justified by the available support (except as indicated). Using OIRM's categorization of controls, the following areas were evaluated:

Organization and Management of OIRM

Twelve controls identified and self-assessed by OIRM personnel were tested by the OIG. In three of the twelve controls, management's assertions were not fully supported:

- "Personnel policies encourage training and development to qualify personnel for their functional responsibilities." The assigned risk rating was low;
- "Formal job descriptions exist and are kept up to date." The assigned risk rating was medium (this may be an appropriate risk rating; however, management's assertion that the control is in place and operating is not fully supported); and
- "Policy manuals and procedure manuals exist and are used by personnel." The assigned risk rating was low.

Application Systems Development

Seventeen controls that were identified and self-assessed by OIRM personnel were not tested by the OIG because the controls were likely to be ineffective for the following reasons:

- Not all systems under development were in the Project Tracking System or had a Systems Analysis and Programming (SAP) request;

- Systems under development in the Database Design and Information Management Group did not require a SAP (or its equivalent), and no development project was under the control of a formal project tracking system;

- Programmers and analysts were not following the systems development life cycle methodology issued by OIRM;

- Programmers and analysts were following outdated standards (the OIRM "Blue Book") to maintain existing systems and develop enhancements;

- Not all programmers were using a CASE (computer aided software engineering) tool to develop and document new systems. The CASE tool that was being used, Design Aid," is outdated. Better CASE tools now exist; and

- Systems Design and Development Group management has stated to us that not all newly developed systems have the proper documentation and controls in place.

Problems with timeliness, budgeting, and effective communications with users further indicated a weak managerial control environment. The following analysis as of November 1997 is derived from data supplied by OIRM's Project Tracking System, which does not reflect all software development and maintenance actions OIRM is currently working on – and does not always reflect accurate project completion data. Therefore, actual performance figures may be better -- or worse -- than indicated below.

- 83.4 percent of active, pending acceptance and completed projects were behind schedule;

- 28.7 percent of active, pending acceptance and completed projects were over budget, by 9.2 to 816.1 percent;

- Of 157 active, pending acceptance and completed projects, the average project length was 37.2 months, but the average number of months budgeted for these 157 projects was 20.1 months; and

- 24.2 percent of 157 active, pending acceptance and completed projects that were over budgeted were also behind schedule, as noted above.

With respect to software projects affecting the financial statements, as of November 1997:

- Forty-eight of the 157 active, pending acceptance and completed projects or 30.6% were owned by the Comptroller;
- Fifteen of these 48 software projects or 31.3 percent were over budgeted by 6.3 to 438.3 percent; and
- Thirty-six of the 48 Comptroller-owned software projects or 75 percent were behind schedule by 1 to 52 months.

The above software development and maintenance statistics for the Office of the Comptroller are of particular concern, especially in light of the fact that the general ledger system -- a key component of the financial management system -- is not yet Year 2000 compliant.

Application Systems Maintenance

Nineteen controls were identified and self-assessed by OIRM. Seventeen of the 19 controls were tested by the OIG. Six of management's assertions could not be fully supported by the evidence, as follows:

- "ADP management authorization and written approval are required for all application systems/program changes." The assigned risk rating was low;
- "Change requests are in writing and include the reasons for the requested changes." The assigned risk rating was low;
- "Approved change requests are required for all changes, and a log is kept of completed changes and changes in process." The assigned risk rating was low;
- "Formally approved written standards for program changes and documentation exist and are followed." The assigned risk rating was low;
- "Application systems changes (program changes, changes in user-department or other manual procedures, etc.) are subjected to comprehensive testing and approval prior to implementation." The assigned risk rating was low; and
- "Testing is performed only on test files." The assigned risk rating was low.

Systems Software Support

Twelve controls were identified and self-assessed by OIRM. The OIG tested the 12 controls. Four of management's assertions could not be fully supported by the evidence, as follows:

- "Authorization and written approval of all modifications are required by ADP management before changes are made." The assigned risk rating was low;

- "There is thorough supervision and review of all changes." The assigned risk rating was low;

- "System programmers are not allowed to operate the computer to implement changes." OIRM management properly indicated that this control was not operating; however, the risk rating assigned was low, which may be unreasonable; and

- "Systems software documentation (whether source or object codes) is physically secure and access is restricted to authorized systems programmers." The assigned risk rating was low.

Computer Operations

Fifteen controls were identified and self-assessed by OIRM. The OIG tested the 15 controls. One of management's assertions could not be fully supported by the evidence, as follows:

> "Active supervision and review are provided on each shift; the supervisor instructs the operators in systems processing activities such as the processing schedule, the programs to be run and the correct dating constants to be used." The assigned risk rating was medium (this risk rating may be appropriate; however, management's assertion that the control is in place and operating cannot be fully supported).

Data Entry Controls

Six controls were identified and self-assessed by OIRM. The OIG tested five of the six controls. Two of management's assertions could not be fully supported by the evidence, as follows:

- "Passwords and access authorization tables are used to restrict use of terminals to authorized personnel for authorized purposes." The assigned risk rating was low; and

- "Computer output and distribution thereof are under strict control of a data control function." The assigned risk rating was low.

The above exceptions are more fully discussed in Findings 3 through 8.

When OIRM personnel attempted to assess the controls, they did not identify or report any material internal control weaknesses, conducted no separate vulnerability analysis prior to its internal control reviews, and prepared no corrective action plans addressing prior outstanding audit findings and recommendations. Some of these issues are elaborated on in Findings 3 and 4 of this report.

Internal control standards are contained in the "OIRM Management Control Review Guide," dated September 20, 1995, which delineates the internal controls required to be in place and operating within OIRM. Also, GPO Instruction 825.18A describes GPO policy, responsibilities, standards, and methodologies to be used in performing internal control evaluations. GPO Instruction 825.16B, *GPO Telecommunications and Automated Information (TAI) Systems Security Program*, as amended on August 26, 1994 also describes GPO policy and procedures regarding the protection of sensitive information.

Further guidance on internal control standards may be found in the second edition of "CobiT: Control Objectives For Information Technology and Related Technology" and "Control Objectives, Controls in an Information Systems Environment: Objectives, Guidelines and Audit Procedures," published in April 1998 and April 1992, respectively, by the Information Systems Audit and Control Foundation.

The cause of inaccurate control self-assessments is: (1) inadequate OIRM management attention, (2) lack of resources, and (3) inadequate evaluation and testing of internal controls before assessing them. OIRM lacked an up-to-date, detailed definition and explanation of internal control objectives and techniques, to include what constituted a material weakness. OIRM also lacked detailed guidance and support on how to perform a vulnerability analysis and implement internal control evaluation, testing, assessing, and reporting.

The effect of not completely and accurately self-assessing all internal controls could provide the Public Printer and other concerned parties (GPO management, the GPO OIG, Congress, the General Accounting Office, external auditors of the financial statements, and the public) with an inaccurate perception of the effectiveness of internal controls within OIRM.

RECOMMENDATION

The Director, OIRM, should reassess internal controls, to include their definitions, as well as the risks associated with a particular control not being in place and operating. Then, OIRM personnel should conduct and document appropriate tests to ensure that controls are functioning effectively (9909-03).

MANAGEMENT COMMENTS

The Director, OIRM, disagreed with Finding 2 as stated in Appendix III of this report. In part, the Director stated,

1. "The finding implies that '*system development activity*' is going on when it is not."

2. "With no further '*in-house development*' CASE (computer aided software engineering) tools are not needed."

3. "The report seems to confuse standard '*maintenance*' requests with development."

4. "The statistics referring to maintenance projects being behind schedule and '*over budgeted*' are incorrect and misleading...."

INSPECTOR GENERAL'S RESPONSE

System development activity was ongoing during the course of this audit, and the findings are still applicable to the OIRM environment beyond traditional in-house developmental activity.

CASE tools provide a host of features beyond facilitating development activity to include capabilities which support making informed decisions on off-the-shelf canned software solutions.

We properly collected statistics referring to the maintenance projects and we stand by the results reported. The methodology was in full conformance with audit and analytical standards. Although OIRM disputes our results, they have had ample opportunity to provide additional information and have not done so.

3. DOCUMENTATION

FINDING

OIRM lacked the appropriate documentation in the following areas:

- There was little or no documentation to confirm that internal control self-assessments had been performed;

- Systems Analysis and Programming (SAP) requests for software maintenance actions were not always filled out;

- OIRM's policies and procedures manuals were outdated and incomplete; and

- System software change approvals were not documented.

For each of the 61 controls reviewed by the OIG, OIRM had not retained documentary testing evidence. Thus, it appears that little or no testing had been performed.

Because SAP requests or its equivalents were not always used when developing or maintaining software, the Project Tracking System, which receives input from the SAP requests, did not reflect all systems under development or maintenance within OIRM. The following 12 new systems under development, as of November 1997, were found to lack the required documentation (SAP requests) and were not under the control of the Project Tracking System:

1. Intranet;
2. GPO Telephone Directory;
3. GPO Directives;
4. Distribution of Electronic Output;
5. Various applications to allow agencies to ride on publications;
6. Macrosoft;
7. Replacement for the Telecommunication Information Management System;
8. PERQUERY Replacement;
9. Engineering Service;
10. Scanning of SF-1;
11. Acceptance of Customer Rider Information from the Web;
12. Customer Agency Request Log;

OIRM personnel also indicated that many small software maintenance requests such as the generation of one-time reports did not have SAP requests and were not under the control of the Project Tracking System. In addition, not all personnel in the Database Design and Information Management Group use the automated Project Tracking System.

The "OIRM Standards and Procedures Manual," (the "Blue Book") dated July 1980, had not been updated and was not current. Moreover, OIRM's "Data Management Procedures," dated October 1994, was still in draft form. Also, the "OIRM Management Control Review Guide," dated September 1995, was incomplete.

Supervision and review of system software changes made by the Technical Support Division within the Data Processing Services Group of OIRM was not documented. Written approval was not given for system software changes; instead, the approval was verbal.

Documentation standards are contained in the "OIRM Management Control Review Guide." The Guide delineates controls to be tested and the methodology for testing them. In addition, the internal control assessments themselves explicitly provide for testing in "Comments/Testing/Documentation."

With respect to documenting program changes, the "OIRM Management Control Review Guide," under "Application Systems Maintenance," is explicit:

- "ADP management authorization and written approval are required for all application systems/program changes;"
- "Change requests are in writing and include the reasons for the requested changes;"
- "Approved change requests are required for all changes, and a log is kept of completed changes and changes in process;" and
- "Formerly approved written standards for program changes and documentation exist and are followed."

In the same OIRM guide, under "Organization and Management of the OIRM," the standard is:

> "Policy manuals and procedure manuals exist and are used by personnel."

And in the section titled "Systems Software Support," it is stated that, "There is thorough supervision and review of all changes."

Instruction 825.18A also describes the policy, responsibilities, methodology and standards for a department's internal control program. This instruction should be updated to reflect the requirement of a soon-to-be released new GAO standard for internal controls, as well as GPO's adoption of an integrated IT controls framework as recommended by the GPO OIG and GPO's external auditors.

In addition, the "Monitoring" section of CobiT provides additional guidance on:

- Documentation;
- Assessing Performance; and
- Reporting Results.

In the "Acquisition and Implementation" area of CobiT, the following control objectives provide guidance with respect to documenting the approval of system software changes:

- System Software Maintenance;
- System Software Change Controls;
- Change Request Initiation and Control;
- Control of Changes; and
- Documentation and Procedures.

The reason internal controls testing was not performed and documented was due to a lack of appropriate management attention and understaffing within OIRM. OIRM also lacked the resources to adequately identify, evaluate, test, document, assess, and report its internal controls. There was no up-to-date, detailed definition and explanation of internal control objectives and techniques, such as can be found in CobiT. In addition, OIRM lacked the detailed guidance and support on how to properly implement internal control evaluation, testing, assessment, and reporting.

The cause of not including all development and maintenance activities under the Project Tracking System was non-compliance with established policies. SAP requests were not completed; therefore, the input documentation was lacking. The reason for not including small maintenance activities under the Project Tracking System was that the programmers and analysts considered to formally document and report the small program changes required of the user was a waste of time.

Policies and procedures manuals were outdated and incomplete due to a lack of management attention and under staffing.

The reason that there was no written approval for system software changes was due to the small size of the Technical Support Division, which fosters close and trusting working relationships among its systems programmers. This, combined with a lack of time on the part of the systems programmers, resulted in undocumented approval of changes to systems software. Also, the fact that the systems software changes were self-documenting through the use of the Systems Management Program (SMP) was a sufficiently mitigating control in the view of OIRM management.

The result of not testing and documenting the internal control self-assessments was to produce inaccurate self-assessments (16 out of 61 control self-assessments appeared to be inaccurate as determined by the GPO OIG. (See Finding 2.) Another result was to provide the Public Printer and other concerned parties (GPO management, the GPO OIG, Congress, and the General Accounting Office, external auditors of the financial statements, and the public) with a possibly inaccurate perception of the effectiveness of internal controls within OIRM.

The effect of not including all systems development and maintenance activities under the Project Tracking System was to preclude OIRM and senior GPO management from effectively planning, controlling, and evaluating all development and maintenance activities, especially with respect to budgetary and time controls. Without the visibility and information available from the formal reporting mechanisms built into the Project Tracking System, management is at an increased risk of allowing projects to go over budget and behind schedule. Effective project management is hindered without the information available from an automated project/engagement information system. The organization thus becomes increasingly susceptible to productivity losses on account of waste and mismanagement.

The potential effect of not updating policies and procedures manuals to reflect proper standards and desired practices could reduce the effectiveness of management planning, control, and evaluation of activities within OIRM. Also, employees were following outdated standards that have not kept pace with organizational changes, changes in technology, and changes in methodology. For example, analysts and programmers in the Systems Design and Development Group were still using the OIRM "Blue Book", which was about 18 years old, as the basis to design, develop, and document systems enhancements. The "Blue Book" was used to purchase new software and maintain existing systems, in spite of the existence of OIRM's newly issued draft "Systems Development Life Cycle (SDLC) Methodology." By following the outdated standards delineated in the "Blue Book" and not following the structured and disciplined practices outlined in the new SDLC methodology, OIRM employees incurred risks in the development, purchase, improvement, and maintenance of software. This software: (1) was not adequately documented; (2) lacked internal controls; (3) required numerous "fixes;" and (4) was, possibly, of poor quality, thereby not fully meeting the needs of users.

The effect of not having documentary evidence of supervision and review over systems software changes could make it difficult for senior OIRM management to: (1) monitor and assess the effectiveness of supervision and review within the Technical Support Division and (2) determine if systems software changes were properly authorized and implemented.

RECOMMENDATIONS

The Director, OIRM, should:

- Test internal controls and retain documentation of such before assessing whether or not a control is in place and operating (9909-04);

- Document all systems development and maintenance activities and include this in the automated project tracking system, to include the developmental activities of the Database Design and Information Management Group and the Telecommunications Group. For small system maintenance activities, OIRM personnel should establish annual "umbrella" SAP requests for systems expecting minor maintenance actions for the year, something OIRM management has already begun on a limited basis (9909-05);

- Update policies and procedures manuals (9909-06); and

- Ensure the personnel in the Technical Support Division, Data Processing Services Group, document-approved changes to systems software and obtain written approval to implement them (9909-07).

MANAGEMENT COMMENTS

The Director, OIRM agreed with the finding and recommendations "…to the extent that additional staffing is made available, with the following exceptions.

1. OIRM's present policy requires the SAP requests *only* for the SDG Division and only for system analysis and programming requests. The instances cited were not performed by SDG and involved loading off-the-shelf software and canned solutions – *no* programming involved.

2. With respect to '*systems software*' this recommendation suggests that the supervisor give himself approval in writing."

INSPECTOR GENERAL'S RESPONSE

Regarding "*systems software,*" we are suggesting that the supervisor go to the next level of supervision in OIRM.

4. OUTSTANDING AUDIT FINDINGS AND RECOMMENDATIONS

FINDING

Sections 7b and 8h of GPO Instruction 825.18A require that managers implement or resolve open audit recommendations. Such action should include a prompt evaluation and determination of the proper actions to take in response to reported audit findings and related recommendations.

Requirements to implement audit recommendations are not unique to GPO. In addition to GPO Instruction 825.18A, standards pertaining to corrective action and other internal control matters are contained in the American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) Number 60, "Communication of Internal Control Structure Related Matters Noted in an Audit."

Moreover, CobiT provides further guidance in the "Planning and Organization" section for external requirements review, and practices and procedures for complying with external requirements. In the "Monitoring" section, follow-up activities are addressed.

As of February 1999, many outstanding audit findings and recommendations pertaining to OIRM had not been implemented. These were recommendations contained in prior OIG audit reports, the 1997 financial statement audit of GPO conducted by KPMG Peat Marwick LLP, and the May 1998 Booz-Allen & Hamilton management audit of GPO. The outstanding findings and recommendations are as follows:

U.S. GPO Office of the Inspector General (OIG)

1. *Security for Mainframe Computer Applications* (Report No. 90-45, dated June 22, 1990).

2. *Formulation of Systems Development Life Cycle Procedures for GPO* (Report No. 91-17, dated December 27, 1990).

KPMG Peat Marwick LLP

Some of KPMG Peat Marwick's management letter comments repeat the prior findings and recommendations made by the OIG and Arthur Andersen, LLP (AA). Of the 19 findings and recommendations made to OIRM by KPMG Peat Marwick LLP in their *Management Letter* (dated September 30, 1997, delivered August 14, 1998, and provided to GPO management in conjunction with the 1997 financial statement audit of

GPO), 15 are grouped into one reportable condition and four are presented as other matters, as follows.

REPORTABLE CONDITION

- Logical Access

1. Maintain Adequate Segregation of Duties (NFR EDP-15). This is similar to prior year AA item #45.

2. Establish, Implement, and Review CA-Top Secret Parameters (NFR EDP-13). This is similar to prior year OIG Report No. 90-45. [Office of Administrative Support]

3. Strengthen Controls and Assign Responsibility for Systems Software Security (NFR EDP-17). This is similar to prior year AA item #46.

4. Restrict Logical Access To Sensitive Data To Authorized Users (NFR EDP-2).

- Application Change Control and Systems Development

5. Improve Controls Over Program Changes (NFR EDP-9).

6. Centralize Coordination Of Program Changes (NFR EDP-6). This is similar to prior year AA item #31.

7. Evaluate Costs and Benefits Of The Purchase Of Commercial Off-The-Shelf Software Packages (NFR EDP-18).

8. Implement A Systems Development Life Cycle (SDLC) (NFR EDP-8). This is similar to prior year OIG Report No.91-17 and AA item #35.

9. Acquire And Install A Software Package To Further Control Changes To ADABAS Applications (NFR EDP-10).

- Service Continuity

10. Develop A "Living" Comprehensive Contingency Plan (NFR EDP-3). This is similar to prior year AA item #3.

- Entity-Wide Security Program

11. Develop a Data Security Plan, Policies, and Procedures (NFR EDP-14). This is similar to prior year AA item #50, which also pertains to the Office of Administrative Support.

12. Develop a Process For Performing Risk Assessment (NFR EDP-19).

13. Implement Background Investigation Process For Technology-Related Positions (NFR EDP-24). This also pertains to the Office of Administrative Support.

14. Develop An Information Technology Strategic Plan (NFR EDP-22). This is similar to prior year AA item #36.

15. Reestablish The IT Steering Committee (NFR EDP-21). This finding can only be implemented with the approval of the Public Printer.

OTHER MATTERS

- EDP - Year 2000

16. Organize Efforts To Correct Year 2000 Problem (NFR EDP-23). This is a Y2K Program Office/GPO-wide finding.

- System Software

17. Develop Written Procedures As Resources Become Available (NFR EDP-12). This is similar to prior year AA item #35.

18. Consider Correcting Any APF Administration Practices, Which Do Not Conform To IBM Standards (NFR EDP-1).

- Miscellaneous

19. Implement GPO Instruction 705.25 on Conducting Periodic Reviews (NFR EDP-7). This also pertains to the Office of Administrative Support.

Booz-Allen & Hamilton

On May 21, 1998, Booz-Allen & Hamilton issued their report entitled *Management Audit of the Government Printing Office.* Most of their IS related findings pertained to OIRM, as follows:

1. GPO's I/T Organization is highly decentralized with limited centralized management leadership, coordination, or oversight (Finding 2). This is related to prior year to KPMG NFR EDP-21 and also applies to the Deputy Public Printer, the Production Department, the Superintendent of Documents, and the Printing Procurement Department;

2. GPO faces substantial business risks due to Year 2000 issues relating to the mission-critical legacy systems (Finding 3). This is related to KPMG NFR EDP-3 and also applies to the Deputy Public Printer and the Y2K Program Office;

3. GPO lacks consistent I/T management processes (Finding 4). This is related to prior year OIG Report No. 91-17, AA item #35, and to KPMG NFR's EDP-22 and EDP-8. The finding also applies to the Deputy Public Printer, the Production Department, the Superintendent of Documents, and the Printing Procurement Department;

4. Information management capabilities are inhibited by GPO legacy systems (Finding 5). This is a GPO-wide finding, which also applies to the Deputy Public Printer; and

5. GPO faces many challenges in maintaining modern technical skills in its I/T workforce (Finding 7). This also applies to the Deputy Public Printer, the Production Department, the Superintendent of Documents, and the Printing Procurement Department.

The reasons that prior audit deficiencies remain uncorrected and that no corrective action plan has been put together and implemented were: (1) an insufficient level of control consciousness within OIRM; and (2) under resourcing of OIRM and the Telecommunications and Automated Information (TAI) Systems Security Group in the Office of Administrative Support.

The effect of not preparing and implementing a corrective action plan to fix control deficiencies could potentially decrease mission performance due to increased susceptibility to fraud, waste, abuse, illegal acts, theft, and mismanagement. Also, GPO could sustain catastrophic data loss, damage, and corruption, as well as suffer cessation of key business functions.

RECOMMENDATIONS

The Director, OIRM, should develop and implement a corrective action plan to resolve all outstanding audit recommendations in conjunction with other GPO departments, when appropriate (9909-08); and

The Director, Office of Administrative Support, in conjunction with OIRM, should develop data security plans, policies, and procedures (KPMG Peat Marwick LLP audit recommendation NFR EDP-14), and implement a background investigation process for technology-related positions (NFR EDP-24) (9909-09).

MANAGEMENT COMMENTS

The Director, OIRM, and the Director, Office of Administrative Support, agreed with the finding and recommendations as stated in Appendix III and Appendix IV of this report. In addition, the Director, OIRM stated,

> "OIRM does not disagree with the IG's recommendations provided that other GPO departments that are responsible cooperate and that the necessary additional staffing is provided."

Also, the Director, OIRM, did take exception to references to outstanding audit findings as pertaining to OIRM. (See Appendix III for the full text of the Director's comments.)

5. APPLICATION SOFTWARE CHANGE CONTROL PROCEDURES

FINDING

Application software change control procedures could be improved. Programmers have access to production jobs while testing software program changes, and they do not always test program changes.

Analysts and programmers in the Systems Design and Development Group within OIRM can access production libraries in the batch mode while testing program changes relating to software maintenance activities. Moreover, not all program changes are thoroughly tested by personnel. Programming changes involving only minor modifications are sometimes not tested.

Internal control standards are contained in the "OIRM Management Control Review Guide, Application Systems Maintenance," which states:

- "Testing is performed only on test files;" and

- "Application systems changes (program changes in user-department or other manual procedures, etc.,) are subjected to comprehensive testing and approval prior to implementation."

The CobiT methodology provides additional guidance. The "Planning and Organization" area in the section entitled Segregation of Duties addresses the issue. And in the "Acquisition and Implementation" section, there is also guidance on software change controls, as follows:

- Testing of Changes;
- Change Request Initiation and Control;
- Control of Changes;
- Parallel/Pilot Testing Criteria and Performance;
- Final Acceptance Test;
- Security Testing and Accreditation; and
- Operational Test.

Testing was inappropriately performed on production libraries and not all program changes were tested because some OIRM programmers and analysts did not always comply with established OIRM policy. They believed that more thorough and effective testing of software programming changes in the batch mode could be done on production files. Also, some programmers and analysts believed that testing was not needed for small, maintenance program changes and that to perform such testing would be inefficient and a waste of time.

Also, the lack of user testing and implementation of adequate configuration management on the part of OIRM management are other reasons analysts and programmers have been accessing production jobs to test program changes while not testing all program changes.

The potential effect of testing software changes in the batch mode against production files could increase the risk of data loss, damage or corruption. The potential effect of not testing all program changes, no matter how small, could increase the risk of putting into place a faulty or poorly performing software program. This could possibly result in the loss, damage, or corruption of data.

RECOMMENDATION

The Director, OIRM, should ensure that programmers only perform program change testing in the test region, and that they test all program changes, no matter how small (9909-10).

MANAGEMENT COMMENTS

The Director, OIRM, agreed with the finding and recommendation.

6. ACCESS

FINDING

Access to the computer system including the reports generated therefrom can be improved.

Some employees retained inappropriate access to the system after they had been transferred to another department within GPO. Employees could also retain inappropriate access if they had been: (1) suspended; (2) put on administrative leave; (3) had their security clearances revoked or suspended; (4) out on extended leave without pay; or (5) not working at GPO on account of collecting workers' compensation. For example, in the review of CA Top Secret access profiles for one GPO department, it was noted that a secretary still retained certain access privileges within this department in spite of her transfer to another department within GPO years ago.

There was no control in place within the Technical Support Division of the Data Processing Services Group, OIRM, to prevent unauthorized or inappropriate access to the system if an individual's employment circumstances within GPO change as described above. OIRM is dependent upon the Office of Personnel, the Comptroller, the Office of Administrative Support, the affected employee, or the employee's supervisor for notification of changes in the employee's employment or clearance status, which does not always happen.

Also, lists authorizing the pick up of computer generated reports from the Production Control Branch of the Data Processing Services Group were outdated. Terminated employees still had the authorization to receive computer reports. For example, in one access list reviewed, dated July 30, 1991, one GPO department showed 16 individuals as requiring access (out of a total of 27 people on the access roster), yet these 16 individuals were no longer part of that department. In fact, 15 of the 16 individuals had left GPO.

GPO Instruction 825.16B, *GPO Telecommunications and Automated Information (TAI) Systems Security Program,* states:

- "It is the policy of the Government Printing Office that Automated Information Systems (AIS) containing sensitive information shall be secured by such means as are necessary to preclude loss, compromise, manipulation, or exploitation, and that all other AIS be provided with adequate levels of security according to the threat or vulnerability."

- "Systems/End users of automated information technology shall ensure that, if appropriate, a GPO Form 2447, Request for Systems Access, is prepared in accordance with GPO Instruction 705.12 for employees being separated, transferred, or reassigned in order that these employee's authorizations to access the GPO Mainframe Computer Facilities can be removed."

With respect to the distribution of computer generated reports, the "OIRM Management Control Review Guide," states, "Computer output and distribution thereof are under the control of a data control function."

CobiT provides additional guidance on access control.

The reason that the OIRM Production Control Branch maintained outdated employee lists was that user departments did not update their lists of employees authorized to receive output from the data center. Also, there was no tickler system in place within the Production Control Branch to periodically alert user departments that their access lists needed updating.

The potential effect of allowing certain employees inappropriate access to the system could increase the risk that programs and data may be lost, damaged, corrupted, or otherwise changed without the authorization of management.

The potential effect of allowing terminated GPO employees access to computer generated output could possibly compromise the security of GPO proprietary and personal employee data. Such compromise could lead to the unauthorized disclosure of or loss of information, violations of the Privacy Act (the provisions of which GPO has elected to follow on a voluntary basis) and an increased susceptibility to computer crime.

RECOMMENDATIONS

The Director, OIRM, should:

- 1) Request the Director, Office of Personnel, to establish procedures to notify the Technical Support Division, Data Processing Services Group, OIRM, and the Chief, Telecommunications and Automated Information (TAI) Systems Security Group, Office of Administrative Support, when an employee is reassigned or promoted within GPO, 2) request the Comptroller to establish procedures notifying OIRM when an employee is placed on extended leave without pay, administrative leave, receives workers compensation or is suspended, and 3) request the Director, Office of Administrative Support, to establish procedures notifying OIRM when an employee's security clearance has been revoked, suspended or downgraded (9909-11);

- Strengthen internal procedures for altering or removing from systems access those GPO employees whose change in clearance or employment status resulted from reassignment or promotion within GPO, extended leave without pay, suspension, extended administrative leave, revocation, suspension or downgrade of a security clearance, or collection of workers compensation (9909-12); and
- Establish a procedure by which OIRM periodically requests from user departments updated lists of those employees authorized to receive computer generated reports, then take appropriate action to update the lists (9909-13).

MANAGEMENT COMMENTS

The Director, OIRM, agreed with the finding and recommendations.

7. TRAINING

FINDING

OIRM does not develop and maintain collective and individual training plans. The training database maintained by the GPO Training and Career Development Branch, Office of Personnel, is incomplete because it is Training Branch policy not to accept non-GPO sponsored training into the database. Also, Training Branch does not always receive documented proof of training from OIRM. Moreover, individual training conducted in Fiscal Years 1996 and 1997 did not appear to meet OIRM's program and control objectives as evidenced by the following:

- The average number of hours of computer related training received in FY96 was 15.2 hours and 28.2 hours in FY97;

- Fifty eight employees or 56.3 percent of OIRM employees received no computer related training in FY96 and 38 employees or 36.2 percent of OIRM employees did not receive any computer related training in FY97;

- Nine OIRM employees lacked training records (training records are established and maintained in the Training and Career Development Branch, Office of Personnel);

- OIRM only expended $21,803 or 33 percent of its training budget of $66,400 in FY96, with an average spending of $212 for each employee; and

- OIRM's training budget was reduced from $66,400 to $49,000 in FY97. In FY97, OIRM expended $28,783 or 59 percent of its training budget of $49,000 with an average spending of $274 for each employee.

With respect to training, the internal control standard in the "OIRM Management Control Review Guide" states, "Personnel policies encourage training and development to qualify personnel for their functional responsibilities."

Control objectives for training are also addressed in the "Planning and Organization" area of CobiT, under the section "Personnel Training."

The cause of OIRM's anomalous training environment is primarily the belief on the part of management that formal training is not needed for certain employees, particularly the computer operators in the Data Processing Services Group. Also, OIRM does not have an overall training program, to include written long and short-range plans on which to base collective and individual training. The reason that the training database is incomplete is that the GPO Training and Career Development Branch, Office of Personnel, does not always receive written proof of training. Also, it is Office of Personnel's policy not to input training received from non-GPO sponsored training sources. However, OIRM management has stated, that, to its knowledge there is little non-GPO-sponsored training within OIRM.

The effect of having deficient training could limit the development of individual knowledge and skills among the professional information systems workforce in OIRM, resulting in GPO not being fully prepared as it strives to meet future challenges. The effect of having an inaccurate training database could misrepresent to GPO managers and employees the type and duration of training received, which could result in employees receiving inappropriate, excessive or no training.

RECOMMENDATIONS

The Director, OIRM, should:

- Develop collective and individual training plans based on short and long range needs. Prepare a training budget based on these plans and funds available (9909-14); and

- Consider appointing a training coordinator with the responsibility of planning, administering, and executing OIRM's training program. Proof of GPO sponsored training should be submitted to the GPO Training Branch. The training coordinator should also ensure all computer-related training, regardless of the funding source, augments OIRM's training database (9909-15).

MANAGEMENT COMMENTS

The Director, OIRM agreed with the finding and recommendations. The Director commented that OIRM: (1) will develop collective and individual training plans after "Y2K"; (2) has appointed a training coordinator; and (3) will deliver training certificates that were paid by the individuals to the GPO Training Branch, provided, "It's Personnel's decision as to whether they will accept these."

8. SOFTWARE USAGE

FINDING

The following software was found to be of no further use according to users and application programmers, yet was still resident on the mainframe:

Systems Software

- EXTRACT/A, Release 1.3
- Decision Analyzer, Release 3.4.1

Software Applications

1. Automated Position System
2. Bindery Cost Calculating System
3. Congressional Record Index System
4. Contingency Status Overtime System
5. Electronic Photocomposition System
6. Employee Incentive Awards System
7. Executive Information System
8. Hazardous Substance Communications System
9. Keystroke Measurement Reporting System
10. Labor Relations Reporting System
11. Obligation Precertification System

These 11 unused software applications were also erroneously described in the systems level documentation (data dictionary) as "operational" when they should have been classified as "retired."

Control objectives for software utilization and management is addressed in the "Planning and Organization" area of CobiT, under the following sections:

- Corporate Data Dictionary and Data Syntax Rules; and
- Relationships.

It is also accepted information management practice to remove from computer memory software that is no longer of use and periodically upgrade those programs considered by their users to be outdated.

The reason unused software was still resident on the mainframe was due to a lack of effective communication between users and OIRM.

The effect of keeping unneeded software is to use disk space that could otherwise be freed up for other tasks. In addition, programmers and analysts could be wasting time and resources on maintaining software that is outdated and no longer of use. Moreover, maintaining redundant software can adversely impact capacity planning and management.

RECOMMENDATIONS

The Director, OIRM, should:

- Validate software currency with users and remove unused systems software from the mainframe along with other outdated and unused software programs. Establish a control procedure incorporating user surveys and identify software that is not or will no longer be of use (9909-16); and

- Change the status of the 11 unused software applications from "operational" to "retired" in the systems level documentation (9909-17).

MANAGEMENT COMMENTS

The Director, OIRM, agreed with the finding and recommendations. The Director further commented on the status of 11 unused software applications to retire that, "One of these was the Inspector General's own system, which was in a state of disuse...."

LIST OF SUGGESTED CONTROL OBJECTIVES

As indicated in Finding 1, we believe OIRM's internal control self-assessment program is incomplete. Except as indicated by [brackets], the following controls as delineated by the Information Systems Audit and Control Foundation (ISACF) do not appear to have been identified and self-assessed:

I. Planning and Organization

Define a Strategic Information Technology (IT) Plan

1. Information Technology as Part of the Organization's Long and Short-Range Plan
2. Information Technology Long-Range Plan
3. Information Technology Long-Range Planning -- Approach and Structure
4. Information Technology Long-Range Plan Changes
5. Short-Range Planning for the Information Services Function
6. Assessment of Existing Systems

Define the Information Architecture

7. Information Architecture Model
8. Corporate Data Dictionary Syntax Rules
9. Data Classification Scheme
10. Security Levels

Determine the Technology Direction

11. Technological Infrastructure Planning
12. Monitor Future Trends and Regulations
13. Technological Infrastructure Contingency
14. Hardware and Software Acquisition Plans
15. Technology Standards

Define the IT Organization and Relationships

16. The Information Services Function Planning or Steering Committee
17. [Organization Placement of Information Services Function]
18. Review of Organizational Achievements, Roles, and Responsibilities
19. Responsibility for Quality Assurance
20. Responsibility for Logical and Physical Security
21. Ownership and Custodianship
22. Data and System Ownership
23. [Supervision]
24. [Segregation of Duties]
25. Information Technology Staffing
26. [Job or Position Descriptions for Information Services Function Staff]
27. Key Information Technology Personnel
28. Contracted Staff Procedures
29. Relationships

Manage the Investment in Information Technology

30. Annual Information Services Function Operating Budget
31. Cost and Benefit Monitoring
32. Cost and Benefit Justification

Communicate Management Aims and Direction

33. Positive Information Control Environment
34. Management's Responsibility for Policies
35. [Communication of Organization Policies]
36. Policy Implementation Resources
37. Maintenance of Policies
38. Compliance with Policies, Procedures and Standards
39. Quality Commitment
40. Intellectual Property Rights
41. Security and Internal Control Framework Policy
42. Issue Specific Policies
43. Communication of IT Security Awareness

Manage Human Resources

44. Personnel Recruitment and Promotion
45. Personnel Qualifications
46. [Personnel Training]
47. [Cross-Training or Staff Backup]
48. Personnel Clearance Procedures
49. Employee Job Performance Evaluation
50. Job Change and Termination

Ensure Compliance with External Requirements

51. External Requirements Review
52. Practices and Procedures for Complying with External Requirements
53. Safety and Ergonomic Compliance
54. Privacy, Intellectual Property, and Data Flow
55. Electronic Commerce
56. Compliance with Insurance Contracts

Assess Risks

57. Business Risk Assessment
58. Risk Assessment Approach
59. Risk Identification
60. Risk Measurement
61. Risk Action Plan
62. Risk Acceptance

Manage Projects

63. Project Management Framework
64. [User Department Participation in Project Initiation]
65. Project Team Membership and Responsibilities
66. Project Definition
67. Project Approval
68. Project Phase Approval
69. Project Master Plan
70. System Quality Assurance Plan
71. Planning of Assurance Methods
72. Formal Project Risk Management
73. Test Plan
74. Training Plan
75. Post-Implementation Review Plan

Manage Quality

76. General Quality Plan
77. Quality Assurance Approach
78. Quality Assurance Planning
79. The Quality Assurance Review of Adherence to the Information Services Function's Standards and Procedures
80. [System Development Life Cycle Methodology]
81. [System Development Life Cycle Methodology for Major Changes to Existing Technology]
82. Updating the System Development Life Cycle Methodology
83. Coordination and Communication
84. Acquisition and Maintenance Framework for the Technology Infrastructure
85. Third Party Implementor Relationships
86. [Program Documentation Standards]
87. Program Testing Standards
88. System Testing Standards
89. Parallel/Pilot Testing
90. [System Testing Documentation]
91. Quality Assurance Evaluation of Adherence to Development Standards
92. Quality Metrics

93. Quality Assurance Review of the Achievement of the Information Services Function's Objectives
94. Reports of Quality Assurance Reviews

II. Acquisition and Implementation

Identify Solutions

95. Definition of Information Requirements
96. Formulation of Alternative Courses of Action
97. Formulation of Acquisition Strategy
98. Third Party Service Requirements
99. Technological Feasibility Study
100. Economic Feasibility Study
101. Information Architecture
102. Risk Analysis Report
103. Cost-Effective Security Controls
104. Audit Trails Design
105. Ergonomics
106. Selection of System Software
107. Procurement Control
108. Software Product Acquisition

Install and Accredit Systems

109. Training
110. Application Software Performance Sizing
111. [Conversion]
112. Testing of Changes
113. Parallel/Pilot Testing Criteria and Performance
114. [Final Acceptance Test]
115. [Security Testing and Accreditation]
116. [Operational Test]
117. Promotion to Production
118. Evaluation of Meeting User Requirements
119. Management's Post-Implementation Review

Managing Changes

120. [Change Request Initiation and Control]
121. Impact Assessment
122. [Control of Changes]
123. [Documentation and Procedures]
124. Authorized Maintenance
125. Software Release Policy
126. Distribution of Software

III. Delivery and Support

Define Service Levels:

127. Service Level Agreement Framework
128. Aspects of Service Level Agreements
129. Performance Procedures
130. Monitoring and Reporting
131. Review of Service Level Agreements and Contracts
132. Chargeable Items
133. Service Improvement Program

Manage Third Party Services

134. Supplier Interfaces
135. Owner Relationships
136. Third-Party Contracts
137. Third-Party Qualifications
138. Outsourcing Contracts
139. Continuity of Services
140. Security Relationships
141. Monitoring

Manage Performance and Capacity

142. Availability and Performance Requirements
143. Availability Plan
144. Monitoring and Reporting
145. Modeling Tools
146. Proactive Performance Measurement
147. Workload Forecasting
148. Capacity Management of Resources
149. Resources Availability
150. Resource Schedule

Ensure Continuous Service

151. IT Continuity Framework
152. IT Continuity Plan Strategy and Philosophy
153. IT Continuity Plan Contents
154. Minimizing IT Continuity Requirements
155. Maintaining the IT Continuity Plan
156. Testing the IT Continuity Plan
157. IT Continuity Plan Training
158. IT Continuity Plan Distribution
159. Critical IT Resources
160. Wrap-up Procedures
161. User Department Alternative Processing Backup Procedures
162. Backup Site and Hardware

Ensure Systems Security

163. Manage Security Measures
164. [Identification, Authentication and Access]
165. Security of Online Access to Data
166. User Account Management
167. Management Review of User Accounts
168. User Control of User Accounts
169. Security Surveillance
170. Data Classification

171. Central Identification and Access Rights Management
172. Violation and Security Activity Reports
173. Incident Handling
174. Re-Accreditation
175. Counterparty Trust
176. Transaction Authorization
177. Non-Repudiation
178. Trusted Path
179. Protection of Security Functions
180. Malicious Software Prevention, Detection and Correction
181. Firewall Architecture and Connection with Public Networks
182. Protection of Electronic Value
183. Cryptographic Key Management

<u>Identify and Attribute Costs</u>

184. Chargeable Items
185. Costing Procedures
186. User Billing and Charge back Procedures

<u>Educate and Train Users</u>

187. Identification of Training Needs
188. Training Organization
189. Security Principles and Awareness Training

<u>Assist and Advise IT Customers</u>

190. Help Desk
191. Registration of Customer Queries
192. Customer Query Escalation
193. Monitoring of Clearance
194. Trend Analysis and Reporting

Manage the Configuration

195. Configuration Reporting
196. Configuration Baseline
197. Status Accounting
198. Configuration Control
199. Unauthorized Software
200. Software Storage

Manage Problems and Incidents

201. Problem Management System
202. Problem Escalation
203. Problem Tracking and Audit Trail

Manage Data

204. Data Preparation Procedures
205. Source Document Authorization Procedures
206. Source Document Data Collection
207. Source Document Error Handling
208. Source Document Retention
209. [Data Input Authorization Procedures]
210. [Accuracy, Completeness and Authorization Checks]
211. [Data Input Error Handling]
212. [Date Processing Integrity]
213. [Data Processing Validation and Editing]
214. [Data Processing Error Handling]
215. Output Handling and Retention
216. [Output Distribution]
217. Output Balancing and Reconciliation
218. Output Review and Error Handling
219. Security Provision for Output Reports
220. Protection of Sensitive Information
221. Protection of Sensitive Information During Transmission and Transport
222. Protection of Disposed Sensitive Information
223. Storage Management

224. Retention Periods and Storage
225. [Media Library Management System]
226. [Media Library Management Responsibilities]
227. Backup and Restoration
228. Backup Jobs
229. Backup Storage
230. Archiving
231. Protection of Sensitive Messages
232. Authentication and Integrity
233. Electronic Transaction Integrity
234. Continued Integrity of Stored Data

Manage Facilities

235. [Physical Security]
236. Low Profile of the Information Technology Site
237. Visitor Escort
238. Personnel Health and Safety
239. Protection Against Environment Factors
240. Uninterruptable Power Supply

Manage Operations

241. [Processing Operations Procedures and Instructions Manual]
242. [Startup Process and Other Operations Documentation]
243. [Job Scheduling]
244. Departures from Standard Job Schedule
245. Processing Continuity
246. [Operations Logs]
247. Remote Operations

IV. Monitoring

Monitor the Process

248. Collecting Monitoring Data
249. Management Reporting
250. Assessing Performance
251. Assessing Customer's Satisfaction

Assess Internal Control Adequacy

252. Internal Control Monitoring
253. Timely Operation of Internal Controls
254. Internal Control Level Reporting
255. Operational Security and Internal Control Assurance

Obtain Independent Assurance

256. Independent Security and Control Certification/Accreditation of IT Services
257. Independent Security and Control Certification/Accreditation of Third Party Service Providers
258. Independent Effectiveness Evaluation of IT Services
259. Independent Effectiveness Evaluation of Third-Party Service Providers
260. Independent Assurance of Compliance with Laws and Regulatory Requirements
261. and Contractual Commitments
262. Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers
263. Competence of Independent Assurance Function
264. Proactive Audit Involvement

V. Networks

Network Management Controls

265. Understanding Management's Objectives
266. Implementation Plan
267. Control Standards for the Network
268. Hardware and Software Control Features

Network Data Controls

269. Database Distribution
270. Network Data Standards
271. Access to Network Data
272. Network Data Review Mechanism

Network Software Controls

273. Software Communications
274. Access to Network Operating System Software

Network Operations Controls

275. Network Operations
276. Hardware and Software Back-Up Provisions
277. Access to Network Processing Facilities
278. Documentation and Training of Network Operations Personnel
279. Network Post-Implementation Review
280. Network Performance Monitoring
281. Network Contingency Operations Plans

Network Data Security Controls

282. Data Encryption
283. Network Security
284. Network Security Reviews

LAN Management Controls

285. Network Management Policies,
286. Network Support and Management
287. Network Change Control

LAN Security Controls

288. Network Logical Security
289. Network Physical Security

VI. Electronic Data Interchange (EDI)

EDI Management Controls

290. Management Objectives
291. Cost-Benefit Analysis
292. Service Supplier Selection
293. Contract Terms

EDI Operations Controls

294. User Identification and Verification
295. Program Protection Controls
296. Application Software Controls
297. User Manual
298. Service Invoices

For those controls denoted in [brackets], the wording of the controls objective provided by ISACF differs, in some respects, with the wording used by OIRM in its control self-assessments. While these particular control objectives are essentially similar, there are differences in scope and terminology. Also, the control objectives listed above are derived from a framework and set of standards that OIRM has not yet adopted.

OTHER MATTERS DISCUSSED WITH MANAGEMENT

Position descriptions existed for all established positions (filled and unfilled), but they were outdated, incomplete, and, in some cases, duplicative or very similar. We consider many of the position descriptions to be outdated, because of the fast changing nature of the information technology field. There were also six unestablished positions being filled in OIRM for which no position descriptions existed.

There were 71 position descriptions for which there were vacancies. The age of all the position descriptions ranged from about 21 years old (the position description was written in September 1977) to almost six years old (the position description was written in December 1992). As compiled from data maintained by the Position Management Branch in the Office of Personnel, the range of ages for each type of job position vacancies is as follows:

Position Title	Series/Grade	Number Of PD's	Age of Oldest PD	Age of Newest PD
Secretary (Typing)	PG-318-04-09	10	17 yrs., 6 mos.	8 yrs., 8 mos.
Clerk Typist	PG-0322-03/04	2	13 yrs., 5 mos.	12 yrs., 8 mos.
Communications Clerk	PG-0394-03	3	13 yrs.	10 yrs., 6 mos.
Data Transcriber	PG-0356-04	1	20 yrs., 11 mos.	Same
Computer Clerk	PG-0335-02-04	4	14 yrs., 3 mos.	8 yrs.
Control Clerk	PG-0303-02/03	2	10 yrs., 5 mos.	9 yrs., 11 mos.
Computer Asst.	PG-0335-05-11	8	17 yrs., 6 mos.	14 yrs., 3 mos.
Lead Computer Asst.	PG-0335-10	1	15 yrs., 10 mos.	15 yrs., 10 mos.
Supvy. Computer Asst.	PG-0335-11/12	3	19 yrs., 8 mos.	19 yrs., 8 mos.
Computer Operator	PG-0332-03-06	6	18 yrs., 1 mo.	19 yrs., 8 mos.
Supvy. Computer Op.	PG-0332-11/12	3	20 yrs., 4 mos.	20 yrs., 4 mos.
Computer Specialist	PG-0334-05-14	21	15 yrs., 11 mos.	8 yrs., 9 mos.
Supvy. Computer Spec.	PG-0334-14	5	14 yrs., 11 mos.	5 yrs., 6 mos.
Supvy. I/S Spec.	PG-0301	1	Unknown	Unknown
Telecom Systems Instal	KA-2501	1	8 yrs., 1 mo.	8 yrs., 1 mo.

OIRM management and the Position Management Branch, Office of Personnel, had not analyzed current requirements in OIRM.

Moreover, position descriptions do not yet exist for the following:

- Webmaster;
- Network Engineer;
- LAN Administrator; or
- Database Administrator.

To address the above, OIRM might request the Office of Personnel to conduct an audit of OIRM's position descriptions to determine the accuracy, appropriateness, and currency of OIRM's filled and unfilled position descriptions. Upon completion of the position description audits and with the assistance of the Office of Personnel, OIRM, might further analyze current job requirements, eliminate duplication, and then update or, where applicable, create new position descriptions, when warranted.

UNITED STATES GOVERNMENT

memorandum

DATE: August 31, 1999

REPLY TO ATTN OF: Director, Office of Information Resources Management

SUBJECT: **IG Draft Report on Management Control Program, Dated July 15, 1999**

TO: Inspector General

Results in Brief

The internal control assessment and testing policy was officially implemented at the GPO just recently on May 28, 1997 by GPO Instruction 825.18A, ***Internal Control Program***, with little guidance and no training with respect to the program. No additional staffing was provided to implement it. The design, development, and administration of an internal control program of the magnitude recommended by this report will require a full-time staff of several, and the approval of additional FTEs. Over the past decade, OIRM's staffing levels have been cut by 90 percent from 180 to less than 100. We no longer have "*staff*" positions as such. Due to FTE limitations, these positions were never filled when vacated. OIRM's staff consists of programmers, analysts, computer specialists, and a few "*hands on*" operational managers. It is impossible to develop, implement, and administer internal controls as recommended in this report with present staffing levels. To do so would seriously impair our ability to support the Agency's mission critical systems, particularly with our additional burden of Y2K readiness and remediation for the balance of the year. It is not possible to reassign people from their operational roles at this time without negatively impacting the Agency's mission critical systems.

We disagree with your reference to "*lack of adequate management attention*" as one of "*the primary causes behind OIRM's inability to correct long-standing audit deficiencies and fully implement the GPO internal control program*". There is only one long-standing audit recommendation that is still applicable and the implementation of that is not possible with present staffing levels. The inability to implement a fully comprehensive Internal Control Program is due not to management's inattention, but the lack of requisite staffing to do so, particularly with the additional workload necessitated by Y2K reporting, remediation, testing, and validation.

Removal of unused and outdated mainframe software referred to a handful of customer packages, one of which was the Inspector General's. While OIRM can remind customers that a system is not being used, the responsibility lies with the customer to request the discontinuance of software packages.

The report erroneously and incorrectly states (**Background**, page 4) *that "OIRM agrees to consider adopting the framework delineated in CobiT*" in response to a recommendation made by KPMG. Nothing could be further from the truth as OIRM's previous memoranda will substantiate. The KPMG finding suggested that "*OIRM look to CobiT for guidance in developing*". This is a far cry from stating that we agreed to adopt it.

You indicated that OIRM had "*prepared internal control assessments,*" that we had "*identified and self-assessed the six major areas involving 81 controls.*" However, you then state that, "*no vulnerability assessments were performed.*" We don't understand the distinction between "*internal control assessments,*" which we did and the "*vulnerability assessments*" which you said we did not do. The distinction between the two was not made by the auditor either.

9/1/99

We concur with the OIG's conclusion that their findings cannot be implemented without "*proper staffing of OIRM,*" and that inadequate staffing is the primary cause behind OIRM's inability to correct certain audit deficiencies.

Pages 10 – 13

<u>IG Finding 1</u>: Internal control self-assessment program is incomplete.

<u>IG Recommendation</u>: Adopt a new control framework as delineated in second edition of CobiT, or a generally accepted framework (01).

<u>IG Recommendation</u>: Update OIRM MCR Guide and perform internal control assessments that have not yet been evaluated (02).

MANAGEMENT COMMENTS TO DRAFT.

The report states (page 7) that "*the audit was conducted... and was performed in accordance with generally accepted government auditing standards (GAGAS)..., as well as standards promulgated by the Information Systems Audit and Control Association (ISACA). These ISACA standards are COBIT (Control Objectives for Information and Related Technology)*". The report further states (page 7) that "*...CobiT was used as one criterion to assess OIRM's controls, because OIRM has not adopted a similar framework to guide its internal control revisions*". Your report goes on to state (page 8) that you use various other (COSO) control standards.

Thus, your report evaluates OIRM's Management Control Program (MCP) using the above criterion, which is not applicable to GPO.

However, the OIRM has developed its internal controls using the ***ARTHUR ANDERSON's Guide for Studying and Evaluating Internal Controls in the Federal Government.*** The GPO IG's staff advised this functional approach. It covers most of OIRM's functions. Moreover, our MCP supports the current Federal Government internal control philosophy as expressed in:

- *Federal Managers – Financial Integrity Act of 1982.* This Act required Federal managers to establish internal controls. It is the founding legislation for internal controls.

- ***OMB Circular A-123, as revised June 21, 1995.*** This revision simplified this Circular. This Circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls. The Circular did not use the COSO framework stating that the Circular virtually incorporates all its concepts in terms meaningful to the Federal manager.

For the most part, OIRM believes our control framework is adequate. Many of the six major areas and resultant 42 high-level controls either are assigned to other GPO organizations, or are not appropriate at GPO.

Please withdraw this finding and recommendations, and the entire Appendix 1 (List of Suggested Control Objectives). Please delete all references to COBIT in the report as they do not apply to the Federal Government or GPO.

OIRM cannot adopt a comprehensive control framework to the level of detail and specificity required by "*CobiT*" with its present staffing levels. The GPO should not follow "*CobiT*" which was not designed for the Federal Government, is not used by other Federal Agencies, and is not mandatory.

Predicated on the above, OIRM cannot implement the first part of the recommendation, and disagrees with the second part.

Pages 14 - 18

IG Finding 2 – Accuracy of Internal Control Self-Assessments (Reviews)

IG Recommendation – ***The Director, OIRM should reassess internal controls, to include their definitions, as well as the risks associated with a particular control not being in place and operating. Then, OIRM personnel should conduct and document appropriate tests to ensure that controls are functioning effectively.*** (Who's definitions are referred to above?)

OIRM disagrees with the finding, as follows:

1. The finding implies that "*system development*" activity is going on when it is not. No new systems will be developed in-house as recommended by both KMPG and Booz-Allen. All future systems will be off-the-shelf canned solutions.

2. With no further "*in-house development*" CASE (computer aided software engineering) tools are not needed.

3. The report seems to confuse standard "*maintenance*" requests with development.

4. The statistics referring to maintenance projects being behind schedule and "*over budgeted*" are incorrect and misleading. The data used is old and was not properly collected. OIRM's customers/users control their own priorities and the details of their individual maintenance requests. Maintenance requests are often superceded by more important ones or emergency systems support.

Pages 19 – 23

IG Finding 3 – Documentation.

IG Recommendation – ***Test internal controls and retain documentation of such before assessing whether or not a control is in place and operating.***

IG Recommendation – ***Document all systems development and maintenance activities and include this in the automated project tracking system, to include the developmental activities of the "umbrella" SAP requests.***

IG Recommendation – ***Update policy and procedures manuals, and***

IG Recommendation – ***Ensure personnel in the Technical Support area, DPSG document approved changes to systems software and obtain written approval to implement them.***

The OIRM agrees with these recommendations to the extent that additional staffing is made available with the following exceptions.

1. OIRM's present policy requires SAP requests *only* for the SDG Division and only for system analysis and programming requests. The instances cited were not performed by SDG and involved loading off-the-shelf software and canned solutions – *no* programming involved.

2. With respect to "*systems software*", this recommendation suggests that the supervisor give himself approval in writing.

Pages 24 – 27

Finding 4 – Outstanding Audit Findings and Recommendations.

IG Recommendation – The Director, OIRM, should implement or otherwise resolve all outstanding audit recommendations in conjunction with other GPO departments, when appropriate.

IG Recommendation – The Director, Office of Administrative Support, in conjunction with OIRM, should develop data security plans, policies, and procedures, and implement a background investigation process for technology-related positions.

OIRM does not disagree with the IG's recommendations provided that other GPO departments that are responsible cooperate and that the necessary additional staffing is provided. However, any references to "*many*" outstanding audit findings and recommendations pertains to OIRM is false and misleading as follows:

1. Only two findings are older than one year:

   a) Security for Mainframe Computer Applications (Report No. 90-45, June 22, 1990). This refers to the Office of Administrative Support, not OIRM.
   b) Formulation of Systems Development Life Cycle Procedure for GPO (Report No. 91-17, December 27, 1990). A 1,000-page SDLC was developed by OIRM at that time, but it was never approved for official issuance by GPO. This is obsolete and not meaningful when *no* future systems will be developed as directed by Booz-Allen and KPMG. Off-the-shelf "*canned software*" will be used by OIRM.

2. The KPMG finding is erroneously and misleadingly mislabeled, ***Management Letter (dated September 30, 1997).*** The management letter was dated August 14, 1998, although it covered the 1997 financial statements. These findings are not a year old. Many have been implemented, many pertain to organizations other than OIRM, and others cannot be implemented until after Y2K, and additional staffing is provided.

Also, the following comments on the reportable conditions cited by KPMG, are offered:

- **Logical Access**

  Numbers 1, 2, and 3 pertain not to OIRM, but to the Office of Administration (these are security issues.

- **Application Change Control**

No. 5: Improve control over program changes.

DONE.

No. 6: Centralize coordination of program changes.

DONE.

No. 8: Implement a Systems Development Life Cycle (SDLC). Not applicable for off-the-shelf software deployment. However, should others feel that an SDLC should be written before acquiring off-the-shelf solutions, then this should be directed to GPO's Policy Coordination or Planning staffs, who are responsible for formulating and writing GPO policy. Such a policy would apply to other GPO organizations as well, such as Prcduction, Printing Procurement, and Documents.

- **Entry-Wide Security Program**

No. 11: Does not apply to OIRM. The responsibility belongs to Office of Administrative Services.

No. 13: Does not apply to OIRM. The responsibility belongs to Office of Administrative Services.

No. 14: Develop an "*Information Technology Strategic Plan*". This has been done for OIRM and the Office of Planning has produced a draft 5-year plan for the GPO.

No. 15: Reestablish the IT Steering Committee. OIRM coordinates its activities and projects across many organizations.

Progress has been made in spite of the all-consuming Y2K effort and the 90 percent reduction in OIRM's staff over the last decade. Also, eight of the 19 conditions are the responsibility of other organizations.

Pages 28 - 29

IG Finding 5 – Application Software Change Control Procedures Could be Improved.

IG Recommendation ***– The Director, OIRM, should ensure that programmers only perform program change testing in the test region, and that they test all program changes, no matter how small.***

OIRM agrees with the recommendations and this has always been our policy.

Pages 30 – 32

IG Finding 6 – Access: Retaining Inappropriate Access to System After Change in Employment. Authorization Lists for Pick Up of Computer Reports Outdated.

IG Recommendation – Request Director, Office of Personnel, to establish procedure to notify OIRM and Office of Administrative Support, when an employee is reassigned or promoted with GPO, and request Comptroller establish procedures notifying OIRM when employee is on extended leave without pay, administrative leave, workers compensation, or is suspended. Request Office of Administrative Support establish procedures to notify OIRM when employee's security clearance has been revoked, suspended, or downgraded.

IG Recommendation – Strengthen procedures for altering or removing from systems access those GPO employees whose change in clearance or employment status resulted from reassignment or promotion with GPO, extended LWOP, suspension, extended administrative leave, revocation, suspension or downgrade of a security clearance, or worker's compensation.

IG Recommendation – Establish procedure by which OIRM periodically requests from user departments updated lists of those employees authorized to receive computer generated reports, then take appropriate action to update the lists.

OIRM agrees with these recommendations.

Pages 33 - 34

IG Finding 7 – Training Problems.

IG Recommendation – Develop collective and individual training plans based on short and long range needs. Prepare a training budget on these plans and funds available.

OIRM concurs and will fully implement after Y2K.

IG Recommendation – Appoint training coordinator to administer OIRM training program.

DONE.

IG Recommendation – Copies of training certificates should be submitted to GPO Training Branch.

This refers to training paid for by the individual. It is Personnel's decision as to whether they will accept these.

OIRM's Comments on the Inspector General's Findings on Training are as Follows:

- No evidence has been provided to support the statistics for average number of hours of training, i.e., 15.2 hours for FY96 and 28.2 hours for FY 97. In fact, perhaps OIRM should be commended for almost doubling (90 percent increase) in training from 1996 to 1997. OIRM management has been vigorous in expanding and encouraging IS training in order to keep abreast of the latest technology. Although some efforts have been put on hold (out of necessity) until Y2K is complete, a vigorous effort will begin after Y2K remediation, testing, and validation are completed.
- We disagree with the numbers shown for percent of OIRM employees receiving training and no specificity was provided to support them.

- OIRM requests a clarification of GPO's policy on training when no new technology is being introduced. That is, should all employees receive some training, no matter what it is or whether it is needed or not? Are you recommending training for "the sake of training"?

- Our training expenditures are significantly less than what was actually the case because the Office of Personnel arranged many classes for OIRM. When training is taken at GPO, the cost is absorbed by GPO, not OIRM. In this case we are being criticized for our attempts to save money by working with the Office of Personnel to effect savings.

- Also, it should be noted that the Office of Personnel maintains an excellent up-to-date electronic database of training for each employee, which includes both in-house and outside training.

Pages 35 – 36

IG Finding 8 – Software Usage.

***IG Recommendation** – Validate software currency with users and remove unused systems software from the mainframe along with other outdated and unused software programs. Establish a control procedure incorporating user surveys and identify software that is not or will no longer be of use.*

OIRM concurs. This has been done.

***IG Recommendation** – Change the status of the 11 unused software applications from operational to retired in the systems level documentation.*

OIRM concurs. This has been done. One of these was the Inspector General's own system which was in a state of disuse for several years.

SUMMARY

In summary, given unlimited time and resources, most of the recommendations could be implemented. However, a control program to the extent specified by the often referred to "*CobiT*" standards would be cost prohibitive in terms of the additional staffing that would be required to establish, monitor, and administer it.

PATRICIA R. GARDNER

U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF ADMINISTRATIVE SUPPORT

memorandum

DATE: August 3, 1999

REPLY TO
ATTN OF: Director, Office of Administrative Support

SUBJECT: Draft Report on the Management Control Program within OIRM

TO: Inspector General

We have reviewed your draft audit report on the Management Control Program within the Office of Information Resources Management (OIRM), dated July 15, 1999, and concur with your findings and recommendations as they relate to the Office of Administrative Support.

Thank you for the opportunity to comment.

R.J. GARVEY

Appendix V
Page 1 of 1

INSPECTOR'S GENERAL RESPONSE

In response to the Director's, OIRM, comments concerning the Results in Brief:

OIRM management disagreed with our report language ***"lack of management attention"*** as one of the causes of an inadequate internal control program in OIRM. While we appreciate the impacts of Y2K efforts and constrained staffing conditions in OIRM, management still has an inescapable fiduciary responsibility to provide good stewardship of the information assets under its control through an adequate system of management controls.

Management disagreed with our wording on page 4, "***...OIRM agrees to consider adopting the framework delineated in CobiT...."*** On April 28, 1998, OIRM management signed and concurred with the KPMG Notification of Findings and Recommendations (NFR) which recommended the use of CobiT.
Albeit that the focus of the recommendation was on security, many other related controls were also addressed. The operative word in our recommendation is "*consider*".

Management commented that ***"We don't understand the distinction between internal control assessments and vulnerability assessments"***. Please refer to GPO Instruction 825.18A

UNITED STATES GOVERNMENT

memorandum

DATE: September 2, 1999

REPLY TO ATTN OF: Director, Office of Information Resources Management

SUBJECT: **Status of Internal Control Reviews**

TO: Inspector General

In response to your memorandum of August 27, 1999, due to Y2K remediation, no control reviews were performed this year.

PATRICIA R. GARDNER

RGA
9/7/c