Department of
Veterans Affairs

Office of Inspector General

AUDIT OF
THE INTEGRATED FUNDS DISTRIBUTION, CONTROL POINT ACTIVITY, ACCOUNTING, AND PROCUREMENT (IFCAP) SYSTEM,
PHASE III

IFCAP was performing as designed with the exception of application and data security. The Department is acting to enhance the system to ensure that the application and data are not subject to inappropriate use or destruction.

REPORT No. 7AD-GO7-065
Date: March 28, 1997

Office of Inspector General
Washington DC 20420

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington DC 20420

Memorandum to:

Assistant Secretary for Management (047/90)
Veterans Health Administration Chief Financial Officer (17/105E)

Audit of: The Integrated Funds Distribution Control Point Activity Accounting and Procurement (IFCAP) System, Phase III

1. The Office of Inspector General (OIG) contracted for this audit to be performed to determine whether the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement System (IFCAP), as installed at selected Veterans Health Administration (VHA) sites, is performing as designed; security procedures are adequate to prevent inappropriate use, destruction, disclosure, or modification of the system and/or data within it; backup procedures are adequate to allow manual processing during any downtime and permit complete recovery and updating of appropriate system files upon return of the system; and assess whether installation of site modifications interfere with system requirements and/or controls. IFCAP is an automated system which supports a variety of administrative activities in medical centers. IFCAP is classified as a sensitive system and is used in the management and tracking of most of the $17 billion in VA funds allocated to medical care.

2. This is the last in a series of three audits to determine whether IFCAP is being designed, developed, and implemented in accordance with the requirements and standards for sensitive systems. Phase I evaluated the general, administrative and application/accounting controls designed into IFCAP.[1] Phase II was performed to determine whether information technology controls over the IFCAP development process and the development environment were adequate and complied with required standards.[2] Phase III reviewed the system as installed at seven sites. The seven Department of Veterans Affairs Medical Centers (VAMCs) were selected to provide a variety of sizes, hardware platforms, geographic locations, and software versions. The audit was

[1] Audit of the Integrated Funds Distribution Control Point Activity Accounting and Procurement (IFCAP) System, Version 3.0, Phase I, Report Number 1AD-GO7-116, September 30, 1991

[2] Audit of the Integrated Funds Distribution Control Point Activity Accounting and Procurement (IFCAP) System, Phase II, Report Number 3AD-G07-183, September 30, 1993

performed under an OIG contract with Abt Associates, Inc. Abt's team included their subcontractors the accounting firm of Coopers and Lybrand.

3. The functionality of the system was reviewed at each site to determine if the system was performing as designed. Information technology controls were examined to determine whether the controls over the computer environment were sufficient to prevent inappropriate access to the hardware or data; whether backup and recovery procedures were adequate to allow complete recovery in the event of an operational failure; and whether locally developed application modifications posed any threat to the integrity of the system or data within it.

4. The team also examined application controls which were related to findings from the Phase I audit of IFCAP. The objective was to determine whether the controls performed by VAMC personnel addressed the Phase I findings. The audit was performed in accordance with generally accepted government auditing standards and included such tests as we deemed necessary. The OIG defined the requirements of the audit, approved the audit plan, monitored the audit, and reviewed the draft report. We agree with the contractor's conclusions and recommendations.

5. The audit found that, at the sites visited, the IFCAP system is performing as designed, with some exceptions and that site installed software modifications do not adversely affect internal controls. However, significant problems exist with the security procedures controlling access to the IFCAP system and data within it, and with backup and recovery procedures. In addition, application maintenance procedures employed at many of the sites visited increase the vulnerability of the system to access and modification without management approval. A summary of the audit's significant findings and recommendations follow:

- Some IFCAP users have the ability to perform two or more of the responsibilities of initiating, recording, reviewing, and approving transactions. This provides the risk that unauthorized transactions may be made and not detected. We recommended that management periodically review user access to prevent this situation or, if the situation cannot be avoided due to staffing levels, that monitoring procedures be established to prevent and/or detect unauthorized transactions from being processed.

- System level security needs to be strengthened to prevent unauthorized individuals from gaining access to IFCAP. We recommended logging failed access attempts, with periodic management review of the logs; disabling devices after 3 to 5 invalid logon attempts; restricting multiple logons for non-patient-care staff; forcing the changing of passwords every 90 days; requiring password lengths to be at least six characters in length; preventing the use of obvious passwords; removing Virtual Management System (VMS) accounts inactivated for more than 30 days; and preventing VMS accounts from having duplicate user identification codes.

- Security administration procedures need improvement to ensure that the level of access does not exceed that necessary to fulfill job responsibilities and has been authorized by the appropriate authorities. We recommended that requests for user access and approval of all requests be documented; subsequent requests for approval be documented; and periodic review of user access to ensure access remains commensurate with job responsibilities.

- Procedures for backup, recovery, and contingency planning need improvement to minimize the impact of system failures. We recommended standards be developed for system backups and data recovery, and the periodic testing of recovery and contingency plans.

- Monitoring procedures need to be improved, to ensure that all transactions between IFCAP and FMS are processed completely and accurately. Appropriate procedures need to be in place to ensure that no transactions are lost or only partially processed. We recommended that appropriate monitoring controls be implemented to ensure that all transactions between IFCAP and FMS are completely and accurately processed.

- Internal controls over the processing of certain transactions need to be strengthened. Current processing allows inventory adjustment transactions to update IFCAP files without prior authorization and diminishes the ability of management to effectively manage inventory. In addition, purchasing agents can authorize and obligate purchase orders processed through the General Supply fund without Fiscal Service review. This restricts the ability of Fiscal Service to approve and manage all financial obligations of the VAMC. We recommended a review of the controls over processing of Inventory Adjustment Forms and General Supply Fund transactions. If a review prior to posting is deemed necessary, IFCAP should be modified to require an automated review prior to updating IFCAP. We also recommended removing inventory totals from the Warehouse Inventory Count Form used by personnel performing inventory inspections and development of an internal suspense file for logging goods received prior to fiscal obligation.

- Locally developed security keys and menu options are not documented. These modified keys and menu options can expand or restrict access to key functions of IFCAP and therefore have the ability to reduce internal controls. We recommended documentation of the purpose and assignment of locally developed menu options and security keys and their periodic monitoring to assure the integrity of internal controls.

- Several VAMCs were deviating from recommended FileMan access settings. These settings over IFCAP files should be reviewed and the use of the utility should be monitored. The FileMan utility provides direct access to IFCAP data files and therefore can be used to make unauthorized changes to critical data without an audit trail. We recommended that management periodically review FileMan access settings to IFCAP files; approve departures from recommended settings; and monitor use of the FileMan utility periodically for appropriateness.

- System features designed to identify modification to IFCAP routines and use of programmer mode should be utilized at all VAMCs. Without use of these features, unauthorized modifications to data and programs can be made without a record of when they were made or who made them. We recommended management restrict access to programmer mode to ISC and IRM staff for which this capability is required in their job functions; and implement formal monitoring controls over use of programmer mode.

6. In addition to the significant findings noted above, several other problem areas, which were outside the scope of the audit, were identified that warrant management's attention. They have been included in the management advisory section of the report:

- IFCAP training needs to be improved to ensure competency in the use of application functions and control features.

- A formal organization should be established to continually communicate known problems, work-around solutions, and best practices while waiting for release of software solutions to erroneous processing in IFCAP.

- Review reporting capabilities within IFCAP and provide additional reporting capability as necessary.

- Consider requiring all VAMCs to install Part 3 of Kernel to improve security over IFCAP files.

- Improve testing practices for IFCAP.

- Remove the ability of users to edit their electronic signature block.

7. The audit concluded that, for the VHA sites reviewed, IFCAP was performing as designed except for security. Management needs to assure that the IFCAP system and data within it are not subject to inappropriate use, destruction, modification, or

disclosure. While local modifications to IFCAP at the sites visited had not affected internal controls, application maintenance procedures at several VAMCs make the IFCAP system vulnerable to the introduction of internal control weaknesses; and, increase the risk that sensitive files may be accessed and modified without management's approval, and that unauthorized modification could remain undetected.

8. The Assistant Secretary for Management concurred with all recommendations. The Under Secretary for Health concurred with all recommendations except one, on which he provided a deferred concurrence. The Under Secretary for Health deferred concurrence on our recommendation to make a series of enhancements to the VMS and Kernel systems' security configuration. He indicated that the enhancements would have to be jointly assessed and agreed upon by the Field Information Resources Management Advisory Council, the Kernel Development Team, the Medical Information Security Service, and IRMFO (Information Resources Management Field Office) Customer Support. He also indicated that "[b]ased on evident justification…the CIO will assure that necessary corrective actions are taken." With this one exception, corrective actions were complete or implementation plans were provided for all recommendations. We consider all these recommendations to be resolved. We will evaluate the actions taken to enhance the security configuration of the VMS and Kernel systems and will also follow-up on the implementation of all resolved recommendations.

For the Assistant Inspector General for Auditing

(Original Signed By:)
MICHAEL SLACHTA, JR.
Deputy Assistant Inspector General for Auditing

TABLE OF CONTENTS

SUMMARY

The Abt Team was retained by the Office of Inspector General (OIG) of the Department of Veterans Affairs (VA) to conduct an audit of the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) system. The audit was performed in three phases, of which Phase III is the subject of this report. The purpose of the work performed during Phase III was to examine the performance of IFCAP and related information technology controls at selected VA Medical Centers (VAMCs). We designed and conducted procedures related to the four audit objectives below in accordance with generally accepted government auditing standards as stated in GAO's "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions" and "Standards for Internal Controls in the Federal Government:"

a) *Objective 1:* Perform such tests as are necessary to determine the system is performing as designed.

b) *Objective 2:* Determine whether security procedures are adequate to prevent inappropriate use, destruction, disclosure, or modification of the system and/or data within it.

c) *Objective 3:* Determine whether backup procedures are adequate to allow for manual processing during any downtime, and the complete recovery and updating of appropriate system files upon the return of the system.

d) *Objective 4:* Assess whether the installation of site modifications interfere with system requirements and/or controls.

We performed our procedures from January 24, 1994 to November 3, 1995 at seven VAMCs across the country. The procedures we performed are outlined in Section IC, Approach and Summary of Results, of this report. The VAMC sites varied in size, the version of IFCAP in use, and the role served by the site in the testing and implementation of IFCAP Release 5.0. The audit approach was designed to satisfy the specific objectives defined by the OIG and was agreed to by the OIG. We also developed audit forms tailored for the scope of the audit which served as the mechanism for identifying and documenting our observations. In general, our approach consisted of conducting interviews with VAMC personnel with responsibilities for the areas under our scope, reviewing documentation in support of our understanding, and performing tests of controls. Our understanding of the procedures and controls in place at the VAMCs we visited were documented in the audit forms; these forms served as a basis for the design and performance of our tests of those procedures and controls.

The results of our audit work and findings identified at each site were summarized and discussed with appropriate VA management at each VAMC. The findings that were observed at a majority of the VAMCs were also summarized and represent our listing of "national" issues. We have grouped our findings into the following two categories.

a) *Internal Controls* - These findings are weaknesses in the internal controls designed in and surrounding the use of IFCAP and include controls surrounding transactions processed in IFCAP, and controls over the computing environment of IFCAP.

b) *Management Advisories* - These findings contribute to the maintenance of a well controlled internal control environment and to the effectiveness with which IFCAP is used by the VAMCs.

During the course of our audit, we did not note any findings which would result in a material weakness or material non-conformance in the VA's systems of internal accounting and administrative control and which should be reported in the VA's FMFIA report. The following matrix summarizes the key areas of our findings and specific areas of concern noted in each area. The detailed findings and recommendations are presented in Section II of this report.

Area of Finding	Areas of Concern
Computer Security	a) Application of computer security policies. b) Development and application of supporting security administration procedures c) Configuration of the technical environment to support stronger internal controls and compliance with existing policies. d) Documentation of IFCAP menu options and security key capability.
Change Management Over IFCAP	a) Authorization and monitoring of changes made to IFCAP files.
Data Backup and Recovery	a) Frequency of the performance of system backups. b) Testing of system recovery capability.
Application Controls	a) Reconciliation of IFCAP transactions interfaced with FMS. b) Separation of duties among IFCAP users. c) Consistency of users job responsibilities with access capability within IFCAP. d) Controls to ensure the completeness, accuracy and authorization over certain transactions.

SECTION I:

Introduction

SECTION I: INTRODUCTION

A. PURPOSE

In 1989, the Abt Team was retained by the Office of Inspector General (OIG) to conduct an audit of IFCAP in three distinct phases. Phase I of the audit focused upon IFCAP General/Administrative and Application/Accounting Controls within IFCAP Release 3.0. Phase II centered on information technology controls (IT), including controls over the development process of IFCAP Release 4.0. Phases I and II were completed during 1989 through 1993 and separate reports have been issued for each of these phases. Phase III, the current phase and the subject of this report, addressed the performance of IFCAP and related IT controls at selected VA Medical Centers (VAMCs).

The following four objectives applied to Phase III:

a) *Objective 1:* Perform such tests as are necessary to determine the system is performing as designed.

b) *Objective 2:* Determine whether security procedures are adequate to prevent inappropriate use, destruction, disclosure, or modification of the system and/or data within it.

c) *Objective 3:* Determine whether backup procedures are adequate to allow for manual processing during any downtime, and the complete recovery and updating of appropriate system files upon the return of the system.

d) *Objective 4:* Assess whether the installation of site modifications interfere with system requirements and/or controls.

Phase III of the Audit of IFCAP did not constitute a study and evaluation of internal accounting controls, taken as a whole. While findings and recommendations have been presented in this report, no opinion on whether the system meets the objectives of internal accounting control is given.

B. SCOPE

During Phase III of the Audit of IFCAP, several versions of the application were released and placed into operation at the VAMCs we visited. Because of the continuing development of IFCAP and our effort to evaluate the most current functionality in determining whether the system was performing as designed, we performed our procedures against multiple releases of IFCAP. These releases included IFCAP Release 4.0 and 5.0. Our procedures also encompassed the verified patches to these releases. Lastly, new system functionality introduced in IFCAP Release 3.5 and maintained in IFCAP Release 4.0 was also reviewed.

In the performance of our procedures in this area, we tailored our scope to re-examine certain findings from Phase I of the audit. These findings relate particularly to the use of the IFCAP application at the VAMC and the application controls employed by VAMC management personnel. These findings are documented in the Phase I Audit of IFCAP Report (Finding Numbers 5, 8, 9, & 10, and Management Advisories 1, 2, 3, 4, 5, 6, & 7) and were addressed in procedure 6c of Section IC of this report. Application controls performed by VAMC personnel which address the Phase I findings were documented and tested as part of Phase III. A description of these specific application controls is presented in Section III of this report. If the application controls noted did not sufficiently address a Phase I finding, the finding has been included in Section II of this report.

In addition to system functionality, we reviewed information technology (IT) controls over the computer environment in which IFCAP is operated at each VAMC reviewed. IT controls included system security controls, computer operations controls, and application maintenance controls.

System security controls included controls over the operating systems environment (for example, DEC VAX/VMS), and the Kernel and FileMan systems (layered products in which the Decentralized Hospital Computing Program applications, including IFCAP, execute). We also reviewed the configuration of security within the IFCAP application.

Computer operations controls included the backup and recovery procedures employed at each VAMC to ensure the complete recovery and updating of IFCAP files in the event of an operational failure. The VAMCs' disaster recovery and contingency planning practices were also reviewed to determine whether procedures were adequate to ensure continued business processing.

Lastly, controls over application maintenance were reviewed to assess the extent to which site modifications interfered with system requirements and/or controls. Application maintenance controls included controls over the selection of site configuration options; the request for, testing of, and transfer into the live environment of local modifications; and the availability of user documentation and training.

During Phase III of the Audit of IFCAP, we reviewed seven sites over the course of almost two years. The table below summarizes the sites we reviewed, the IFCAP release installed at each site at the time of our review, and their hardware environment.

Sites Reviewed

Site	Dates of Field Work	IFCAP Release*	Date Converted**	Hardware
Houston, TX	1/24/94 - 2/11/94	4.0	N/A	DECVAX
Salt Lake City, UT	3/14/94 - 4/1/94	4.0	N/A	DECVAX
Altoona, PA	4/17/95 - 5/12/95	5.0	4/94 (Alpha)	DOS
Minneapolis, MN	7/24/95 - 8/8/95	5.0	1/95 (Conversion 1)	DECVAX
Long Beach, CA	8/28/95 - 9/8/95	5.0	8/94 (Alpha)	DECVAX
Salem, VA	9/25/95 - 10/6/95	5.0	11/94 (Beta)	DECVAX
West Palm Beach, FL	10/23/95 - 11/3/95	5.0	3/95 (Conversion 1)	DECVAX

* IFCAP release installed during the time in which the Abt Team conducted the review. It should be noted that IFCAP Release 3.5 was not installed at any of the sites selected for review during the time of our fieldwork.

** Date of conversion to IFCAP release 5.0. "Alpha" and "Beta" refer to VAMC testing of the IFCAP release during the development process. "Conversion 1" refers to the first group of VAMCs to implement the IFCAP Release 5.0 once verified.

C. APPROACH AND SUMMARY OF RESULTS

The approach applied during Phase III of the Audit of IFCAP consisted of a multi-step process. We obtained an initial understanding of VA policies and recommended control procedures surrounding the use of the IFCAP application and the VAMC computer environment in which IFCAP operates. We also conducted a pilot review and documented the control procedures in place to address VA policies as well as local VAMC policies. Based upon our understanding gained from these activities, the Abt Team developed and applied procedures which address the four Phase III audit objectives to be performed at all remaining site reviews. These procedures and the results achieved are described in the table below.

PROCEDURES	RESULT
Objective 1: *Perform such tests as are necessary to determine that the system is performing as designed.*	
1. Update our understanding of the current IFCAP version and patches as a basis for evaluating the consistency of the versions running at each site with the latest supported release of IFCAP.	Procedure was completed without exception.
2. Inquire of local site personnel as to the conformance of the software with the latest supported release of IFCAP. Inquire of local site personnel of the patches distributed to, but not implemented by, the VAMCs since the release of the latest installed version of IFCAP.	Procedure was completed without exception.
3. Obtain an understanding of the capability of the current IFCAP release and patches. Assess the control risk/importance of functions implemented since IFCAP version 3.0	Procedure was completed without exception. Significant functions implemented since IFCAP version 3.0 are included in Section IIIA of this report.
4. Obtain an understanding of the IFCAP functions implemented as a result of the concurred findings from Phases I and II of our audit.	Procedure was completed without exception.
5. Obtain an understanding of the manual/user control procedures related to the non-concurred findings from Phases I and II of our audit.	Procedure was completed with exceptions. Manual/user control procedures are included in Section IIIB of this report. Exceptions are included in Section II of this report, Finding Nos. 1 & 5.

PROCEDURES	RESULT
6. Test system functionality for the following areas through inquiry, observation, and examination: a) the high control risk or important functions implemented since IFCAP version 3.0; b) the IFCAP functions implemented as a result of the concurred findings from Phases I and II; and c) the manual/user functions related to the non-concurred findings from Phases I and II.	Procedure was completed with significant exceptions. Exceptions are included in Section II of this report, Finding Nos. 1, 5 & 6.
Objective 2: *Determine whether security procedures are adequate to prevent inappropriate use, destruction, disclosure, or modifications of the key system and/or data within it.*	
7. Review IFCAP security procedures and options established by site personnel to determine whether they promote sound internal control practices and restrict access to system data.	Procedure was completed with significant exceptions. Security procedures observed during our review are included in Section IIIC of this report. Exceptions are included in Section II of this report, Finding Nos. 2, 3, 7, 8, & 9.
8. Review procedures over the granting, modification and termination of user access.	Procedure was completed with exceptions. Security administrative procedures observed during our review are included in Section IIIC of this report. Exceptions are included in Section II of this report, Finding Nos. 2, 3, & 7.
Objective 3: *Determine whether backup procedures are adequate to allow manual processing during any downtime and complete recovery and updating of appropriate system files upon return of the system.*	
9. Review procedures for backup and recovery of system and data files.	Procedure was completed with exception. Backup and recovery procedures observed during our review are included in Section IIID of this report. Exception noted is included in Section II of this report, Finding No. 4.

PROCEDURES	RESULT
10. Review procedures for the storing of backup information including procedures for off-site storage.	Procedure was performed without exception.
11. Review procedures for manual processing of data in the event that automated methods of processing are unavailable.	Procedure was completed with exception. Contingency procedures observed during our review are included in Section IIID of this report. Exception noted is included in Section II of this report, Finding No. 4.
Objective 4: *Assess whether the installation of site modifications interfere with system requirements and/or controls.*	
12. Review procedures for the installation, modification and testing of IFCAP configuration options and software modifications implemented locally.	Procedure was completed with exception. Application maintenance procedures observed during our review are included in Section IIIE of this report. Exception noted is included in Section II of this report, Finding No. 7.
13. Review system options to determine whether the configuration is in compliance with established IFCAP guidelines.	Procedure was completed with exceptions. Application maintenance procedures observed during our review are included in Section IIIE of this report. Exceptions noted are included in Section II of this report, Finding Nos. 7 & 8.
14. Review local software modifications to determine the effect on internal controls.	Procedure was completed without exception.

At the conclusion of each site review, audit findings and recommendations pertaining to that site were discussed with VAMC management personnel. Once all site reviews had been completed, all audit issues were analyzed and assessed with regard to a "national" perspective. The findings and recommendations presented in Section II of this report represent the issues of "national" significance arising from this audit. In general, the findings included in this report pertained to at least three sites.

SECTION II:

Results of Audit

SECTION II: RESULTS OF AUDIT

A. FINDINGS AND RECOMMENDATIONS

This section discusses findings which significantly impact the internal control environment in which IFCAP is operated. These findings are reportable conditions concerning application controls both within, and surrounding the use of, IFCAP, as well as controls over information security, and backup and recovery of data. A summary of findings and the sites where these findings were noted is presented in Appendix E to this report.

The objective of an internal controls structure is to provide management with reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or disposition, and that transactions are executed and recorded in accordance with management's approval. It is the responsibility of the management of the VA to establish and maintain an internal control structure. In fulfilling this responsibility, estimates and judgments by the Medical Information Resources Management Office (MIRMO), the Office of Finance and Information Resource Management (OF&IRM), and the Office of Acquisition and Material Management (OA&MM) are required to assess the expected benefits and related costs of internal control policies and procedures.

Many of the recommendations may be addressed through enhancements to IFCAP and other related systems, while others may be more suited to changes in the procedures applied by system users at the VAMC level. A few of the recommendations, however, may be most appropriately addressed through enhancements to MIRMO or the IRM's policies and procedures. In evaluating the most appropriate approach, consideration should be given to implementing recommendations in the current release as well as in future versions of IFCAP and supporting systems.

1. Ensure That Appropriate Separation Of Duties Is Achieved Over The Initiating, Recording, Reviewing And Approving Of IFCAP Transactions.

IFCAP controls are designed to separate the functions of initiating, recording, reviewing, and approving of transactions among Control Points, Fiscal Service, and Acquisition & Materials Management Service (A&MMS) IFCAP users. We observed, however, several instances in which users possessed access to IFCAP which afforded them the ability to perform two or more of these responsibilities. Specifically, we observed the following:

1. An accountant within Fiscal Service possessed access to the Control Point Official, Accounting Technician, and Funds Distribution menus, as well as the security keys normally granted to the Fiscal Chief. Such access may potentially allow the accountant to distribute funds, and create and obligate requests for expenditures for a control point.

2. One Fiscal Chief possessed the ability to assign A&MMS menus and security keys to other IFCAP users. Granting users the capability to assign access to IFCAP menus and security keys for which that user is not responsible may not ensure that appropriate consideration is given to the assignment of those menus.

3. A Management Analyst within Fiscal Service possessed access to both purchase and obligate authority within IFCAP.

Allowing users the capability to perform combinations of initiating, recording, and approving transactions provides the risk that unauthorized transactions may be made and not detected. Unauthorized transactions which are not prevented or detected may result in misappropriation of VAMC funds.

Recommendation 1:

We recommend that:

1. Management periodically review user access within IFCAP to ensure that the duties of initiating, recording, reviewing, and approving transactions may not be performed by the same individuals.

2. Appropriate monitoring control procedures be established in those instances where conflicts of interest may not be avoided to prevent and/or detect unauthorized transactions from being processed within the system.

Under Secretary for Health's Comments

a) and b) We concur. Representatives from the Offices of the Chief Information Officer (19), Chief Financial Officer (17) and Chief Network Officer (10N) will participate with the Office of Information Management (045) in assessing if a formal directive is required to address conflict of interest issues in the IFCAP application. If a directive is issued, procedures regarding security controls will be included. In the meantime, facility management will be apprised of the finding and recommendation of this audit that relate to identified security problems. These items will be included on the agendas of selected conference calls to the field conducted by Headquarters program offices and the VISN offices.

Planned December 1996

Assistant Secretary for Management's Comments

b) We concur. Agencies are required to establish a level of security commensurate with the risk. Having a known security conflict of interest would mandate a periodic independent review or alternate monitoring control procedure.

There are situations when a conflict of interest is unavoidable. The VHA CFO is responsible for granting site exceptions to established security levels where a conflict exists. We will work with the Washington IRM Field Office (IRMFO) to develop a hard copy report to be used by management officials to identify such instances when an exception is granted. A target date for this report has not yet been determined, but it is viewed as a high priority item that will be accomplished as promptly as possible.

Abt Team's Response

Management's response satisfies the intent of our recommendation.

.

2. Strengthen Operating System Security Controls.

Our review of information technology controls at each VAMC included an analysis of the security software controls currently in place within the operating system environment. We specifically reviewed the DEC VAX/VMS and Kernel systems to determine if the security configuration of these systems provides an appropriate level of control over system data and programs. Our observations are detailed as follows:

a) Failed access attempts are not logged by the Kernel system and/or are not reviewed by management. Repeated access attempts may signify an unauthorized user seeking access to the system.

b) Numerous valid logon attempts are permitted prior to the Kernel system disabling the user's device. Invalid logon attempts may also signify an unauthorized user attempting to gain access to the system. Disabling of a user's device may prevent that device from being used to gain unauthorized access to the system.

c) Multiple logins are allowed for users. Multiple logins present the risk that terminals may be left unattended and limit users' ability to detect unauthorized use of their account.

d) Verify codes (passwords) lifetimes are greater than ninety days, and in some cases, are unlimited. Changing verify codes less frequently than ninety days increases the risk that users may gain knowledge of other users' verify codes.

e) Minimum password lengths of less than six characters are allowed for VMS accounts. Password lengths less than six characters are more likely to be "guessed" by other system users.

f) Obvious passwords (i.e. passwords that our audit software was able to guess) are allowed. Obvious passwords are also more likely to be "guessed" by other system users.

g) Accounts within VMS have been dis-usered, or disabled, but not removed from the system. Dis-usered accounts may be re-enabled and used for unauthorized purposes.

h) Accounts within VMS have duplicate user identification codes (UICs). AUIC identifies a specific account by number. If two users have the same UIC, management is less able to effectively monitor the activity of a particular account.

Appropriate configuration of system level security is crucial to maintaining a protected information systems environment. The absence of strong system level security control increases the risk that unauthorized individuals will gain access to confidential VAMC data and information.

Recommendation 2:

We recommend that the following enhancements be made to the VMS and Kernel systems' security configuration:

a) Log failed access attempts and ensure management review.

b) Disable devices after three to five invalid logon attempts.

c) Restrict multiple logins from users not directly responsible for delivering patient care.

d) Require verify codes to be changed every ninety days within the Kernel system.

e) Require minimum password lengths of at least six characters for VMS accounts.

f) Prevent and/or discourage VMS users from selecting obvious passwords.

g) Remove VMS accounts once dis-usered for more than thirty days.

h) Restrict VMS accounts from sharing UICs.

Under Secretary for Health's Comments

We defer concurrence. All of these systems' enhancements cannot be approved until they are jointly assessed and agreed upon by the Field Information Resources Management Advisory Council (FIRMAC), the Kernel Development Team, the Medical Information Security Service (MISS) and IRMFO Customer Support. The Chief Information Officer (CIO) will take appropriate steps to assure that these groups review OIG's recommendations for system enhancement and provide feedback about implementation feasibility. Based on evident justification for the individual enhancements, the CIO will assure that necessary corrective actions are taken.

Planned December 1996

Abt Team's Response

We suggest that the Office of Inspector General monitor the actions taken on this recommendation.

3. Improve Security Administration Procedures.

During our review, we noted that the administration of user access to the IFCAP application should be improved. Specifically, our observations are as follows:

a) Documentation is not consistently maintained for requests for, and approval of, access to the IFCAP application. Auditability of user access is significantly limited when documentation of access approvals is not maintained.

b) Documentation of approval of additional access to IFCAP is not maintained, also impairing the auditability of user access.

c) Comprehensive periodic reviews of user access privileges are not performed to ensure that user access remains commensurate with job responsibilities.

Effective security administration is an integral function of maintaining a secure information systems environment. The absence of documented approval of all requests for access prevents management from ensuring that user access has been authorized. In addition, the absence of periodic review of user access provides the risk that users may possess access to data files beyond that which is necessary to perform their job responsibilities. As a result, there is an increased risk that program and data files may be subject to manipulation which could adversely affect data integrity and potentially cause disruptions in data processing services.

Recommendation 3:

We recommend the following improvements to VAMC security administration procedures:

a) Documentation of requests for, and approval of, user access to the IFCAP system be maintained to support the review and authorization of all user access.

b) Documentation of approval of all subsequent requests for approval be maintained.

c) Periodic review and approval of user access to ensure that access remains commensurate with job responsibilities.

<u>Under Secretary for Health's Comments</u>

We concur. The Medical Information Security Service (MISS) has provided sound policies, guidelines and suggested practices governing user access to VHA systems and data that fully meet the intent of this recommendation. Numerous efforts are being made at the Headquarters level to encourage full compliance by the facilities with these directives. MISS is working closely with the VISN CIOs in coordinating informational exchanges with the field. For example, MISS will conduct three regional training workshops for information security officers (ISO) responsible for systems security maintenance in the field facilities. Issues raised in this OIG report will be highlighted during these workshops, which will be conducted during the months of August and September, 1996. In addition, the MISS conducts monthly national conference calls, which include participation by all facilities. During the August 19 conference call, OIG's security administration recommendations will be reviewed and discussed and additional discussion will be included on the agendas of other conference calls as required. It is noted that minutes of the conference calls are routinely circulated to all facilities, thereby reinforcing discussed issues.

Planned September 1996 and Ongoing

Abt Team's Response

Management's response satisfies the intent of our recommendation.

4. Improve VAMC Backup, Recovery, And Contingency Planning Procedures.

We noted that several sites do not perform daily incremental backups of IFCAP data files or perform periodic verification of backup tapes to ensure integrity. In addition, we noted that most VAMCs reviewed do not have a completed and tested Disaster Recovery and Contingency Plan that describes the procedures and tasks to be performed in the event of a disruption to critical computer applications.

Given each VAMC's heavy reliance on information technology, and the financial and patient care impact that could result if such technology was not available, it is essential that appropriate plans be implemented to ensure the recoverability and restoration of automated systems and data. Failure to backup system data or develop, implement, and test established disaster recovery procedures presents the risk that critical system data and operations may be unavailable for an unnecessary length of time.

Recommendation 4:

In order to provide assurance that system operations and data may be resumed in an efficient and timely manner in the event of operational failure, we recommend the development of standards governing system backups and data recoverability, and the implementation of these standards at all VAMCs. These requirements should include the appropriate nature and frequency of system backups, the periodic verification of backup tapes for integrity, and the periodic testing of disaster recovery and contingency plan procedures.

Under Secretary for Health's Comments

We concur. Appropriate policies, guidelines and suggested practices have been issued by MISS to field facilities regarding the development and testing of contingency plans. MISS is closely monitoring facility compliance will all aspects of contingency plan implementation and has recently developed an action plan which will bring all facilities into compliance with contingency plan requirements. A survey of all facilities has been completed by the Regional ISOs (as part of their regularly scheduled site visits) to determine levels of compliance with the contingency plan requirements. Survey findings and follow-up actions are being centrally tracked at the National Center for Information Security, and in coordination with the VISN CIOs, monitoring will continue until full compliance by all facilities is realized. An automated contingency planning product that will facilitate the development and updating of contingency plans system-wide is also being considered for purchase, pending adequate funding support. MISS has also discussed the use of VA's Management Studies and Analyses contract with a vendor who can provide supplemental information security services in support of a national contingency plan development, testing, and alternate site strategy. Again, approval of such a contract is dependent upon available funding.

Planned September 1996 and Ongoing

Abt Team's Response

Management's response satisfies the intent of our recommendation.

5. Improve Monitoring Procedures To Ensure That All Transactions Between IFCAP And FMS Are Processed Completely And Accurately.

The interface between the IFCAP and FMS systems provides for transactions to be processed and updated between the two systems on a daily basis. As with any interface, appropriate procedures need to be developed and placed into operation to ensure that all transactions are processed between the two systems. Examples of conditions that occur that require reconciliations to be performed for the IFCAP and FMS interface include differences in the timing of transactions processed, updated and reported by each system, and the rejection of transactions processed between the systems.

We noted that reconciliation procedures to ensure all IFCAP interfaced transactions sent to and received by FMS have been processed and updated accurately and timely, vary among VAMCs. Specifically, we had the following observations:

1. The frequency with which reconciliations are performed ranges from twice a month to daily at VAMCs. As a result, transaction balances in IFCAP may not be accurate at given points in time and therefore, not support effective decision-making.

2. The procedures performed to reconcile IFCAP and FMS balances are felt to be very time consuming and cumbersome by the VAMCs. The time required for performing these reconciliations was reported to have a negative impact on the performance of timely reconciliations.

Recommendation 5:

We recommend that appropriate monitoring controls be implemented to ensure that all transactions between IFCAP and FMS are completely and accurately processed.

<u>Assistant Secretary for Management's Comments</u>

We concur. We will work with VHA to establish appropriate monitoring controls to assure that all transactions between IFCAP and FMS are completely and accurately processed.

<u>Abt Team's Response</u>

Management's response satisfies the intent of our recommendation.

6. Strengthen Controls Surrounding The Use Of IFCAP To Ensure That Specific IFCAP Transactions Are Authorized, And Processed Completely And Accurately.

A well controlled internal controls environment is established and maintained through a combination of manual and automated internal control procedures. We noted several opportunities to strengthen the internal controls over the processing of certain IFCAP transactions. Specifically, we noted the following:

a) IFCAP provides for inventory adjustments to be processed using the IFCAP "Adjustment Approval Form". These inventory adjustments are actually posted at the time the "Adjustment Approval Form" is created within the IFCAP application. Current procedures require the approval of inventory adjustment transactions by an authorized Approving Official and Accountable Officer. However, the IFCAP application actually posts inventory adjustments upon creation of the "Adjustment Approval Form", without any automated approval required. While a manual review of the inventory adjustment form is still possible, this would occur after the inventory adjustments have been posted. As a result, management's ability to manage inventory balances proactively is diminished.

b) Personnel with responsibility for counting inventory are provided with system generated on-hand inventory totals, prior to conducting each planned physical inventory inspection, through use of the "Warehouse - Inventory Count Form." Providing personnel with IFCAP inventory totals prior to a physical inventory inspection reduces the value of an independent verification of balances through physical inspection, and weakens the control over this process. As a result, management's control procedure to rely on physical inspections to verify the accuracy of inventory totals may not be effective.

c) IFCAP transactions processed through the General Supply Fund, including purchase orders, may be authorized and obligated by Purchasing Agents without Fiscal Service review. The absence of a control requiring Fiscal Service approval of General Supply Fund transactions, prior to obligation of the funds, restricts the ability of the Fiscal Service to approve and manage all of the financial obligations of the VAMC.

d) The functionality to automate the recording and tracking of goods ordered and received by a VAMC but not obligated within the system exists in IFCAP as an optional feature which can be used at the discretion of each VAMC. At the stations visited, manual procedures were being used for this process. Without controls designed to ensure that all inventory is identified and reported, the ability of management to accurately report total inventory on hand is reduced.

Recommendation 6:

In order that management may gain additional assurance that all IFCAP transactions are authorized and processed completely and accurately, we recommend the following:

a) A review of the controls over processing of "inventory Adjustment Forms" should be performed to determine the importance to the VA of approving inventory adjustments prior to being posted in IFCAP. If it is determined that approval of inventory adjustments prior to update in IFCAP is important, we recommend IFCAP be modified to require an automated review of these forms prior to update.

b) Inventory totals in IFCAP should be removed from the "Warehouse Inventory Count Form" used by personnel performing physical inventory inspections.

c) A review of the controls over General Supply Fund transaction processing should be performed to determine the importance to the VA of having Fiscal Service review these transactions. If it is determined that Fiscal Service approval of General Supply Fund transactions is desired, we recommend IFCAP be modified to require an automated review of these transactions prior to update.

d) Emphasize the need to use the functionality in IFCAP to record goods received prior to fiscal obligation.

Assistant Secretary for Management's Comments

a) We concur. We have analyzed the situation, the procedure currently in use, and have decided that no change is necessary.

b) We concur. Personnel counting inventory should not have on-hand inventory totals. Resolution of this recommendation may require changes to IFCAP. We will address any required system changes and completion dates with the Washington IRM Field Office and ensure that any required changes are accomplished promptly.

c) We concur. The DAS for Acquisition and Materiel Management is responsible for the Supply Fund and Fiscal Service has no involvement. Again, we will not change current procedures.

d) We concur. We will emphasize to VHA the need to utilize the features in IFCAP which allow the automate tracking of goods delivered before an obligation exists.

Abt Team's Response

Management's response satisfies the intent of our recommendation.

7. Document The Purpose And Assignment Of Locally Developed IFCAP Menu Options And Security Keys.

We noted that VAMCs create security keys and IFCAP menu options to assist in the assignment of access privileges to users. Local security keys are created to limit access to menu options which did not have initial keys and in some cases, "reverse keys" are created to grant access to menu options that would otherwise be secured. Similarly, local menu options are used quite extensively to create unique menus for users throughout the hospital. These menu options usually are "hybrid" menus containing options from multiple menus, or in some cases a standard menu will have options removed to restrict access to those options.

Locally developed security keys and menu options can be used to enhance internal controls over IFCAP. Likewise, modification of standard security keys and menu options can reduce internal controls by increasing access to critical system functions. In situations where security keys and menu options are used to broaden access, there is an increased risk that users may be granted more privileges than is required for them to perform their job functions. This may result in the introduction of weaknesses in internal controls surrounding IFCAP processing.

Recommendation 7:

In order to ensure that locally created security keys and menu options do not introduce weaknesses in the internal controls over IFCAP processing, we recommend VAMC management document and periodically review all locally developed security keys and menu options. In performing this process, VAMC management should place additional emphasis on controlling assignment of those security keys and options with powerful privileges within IFCAP.

Under Secretary for Health's Comments

We concur. This issue will be reinforced during the scheduled regional training workshops that were previously alluded to in this action plan. In addition, MISS will place special emphasis on issues identified in this recommendation during the routinely-conducted facility security site visits that are conducted by the regional ISOs as well as during the monthly conference calls that are conducted by MISS.

Planned September 1996 and Ongoing.

Abt Team's Response

Management's response satisfies the intent of our recommendation.

8. Strengthen Controls Surrounding The Assignment And Monitoring Of FileMan Access To IFCAP Data Files.

The VA FileMan utility provides direct access to IFCAP data files without the use of IFCAP menus and programs. To safeguard against unauthorized changes to IFCAP data, FileMan access restrictions may be established by file and by user. The IFCAP Security Guide recommends FileMan access settings over key IFCAP data files to help ensure data integrity. We noted, however, that several VAMCs had changed the FileMan access settings over several IFCAP files. We also noted that monitoring procedures over the use of the FileMan utility do not exist.

FileMan access settings determine which users have the ability to delete, update and read data within critical IFCAP files. Changes from recommended access controls over IFCAP files provide the risk that users may gain unauthorized access to data, and that data may be subject to unauthorized manipulation.

Recommendation 8:

In order to ensure the integrity of IFCAP data, we recommend that:

a) Management periodically review FileMan access settings to IFCAP data files.

b) Departures from recommended FileMan access settings be approved by appropriate personnel.

c) Use of the FileMan utility be monitored periodically for appropriateness.

<u>Under Secretary for Health's Comments</u>

We concur. As stated in the response to recommendation 1, representatives from the Offices of the Chief Information Officer, the Chief Financial Officer and the Chief Network Officer will meet to determine whether or not a formal VHA directive should be issued to address a wide variety of information security issues. Items included in this recommendation will also be incorporated into that proposed directive. In addition, however, MISS will place added emphasis on the review of FileMan access settings and associated documentation while conducting scheduled facility security site visits. Medical facility staff will also be apprised of OIG's recommended actions during the upcoming training workshops and monthly national conference calls.

Planned September 1996 and Ongoing

<u>Abt Team's Response</u>

Management's response satisfies the intent of our recommendation.

9. Improve Access Controls And Monitoring Procedures Surrounding Programmer Access to IFCAP.

MIRMO policy states that VAMCs are not permitted to make local changes to IFCAP routines. We noted that Information Resource Management (IRM) staff as well as Information Systems Center (ISC) staff possess the security keys and menu options to access "programmer mode." Users with "programmer mode" access possess the privileges to modify IFCAP routines and data at the VAMCs. We also noted that system features designed to identify modifications to IFCAP routines and use of "programmer mode" are not being utilized by VAMCs. We had the following specific observations surrounding controls over "programmer mode" access:

a) Formalized monitoring procedures over the use of "programmer mode" access do not appear to exist at VAMCs. Access logs can be produced that identify all users that have entered "programmer mode", however these logs are not formally reviewed by management to ensure appropriate use of these privileges. In addition, a programmer with appropriate privileges and access to the VMS operating system can bypass the logging of "programmer mode" access.

b) When programmer access is granted, the system configurations at most VAMCs will restrict programmer access to a specific function within a VAMC without assigning access to all functions at the VAMC. Kernel option PART 3 is a feature that can be used to restrict programmer access to specific files at the VAMC. This feature of the Kernel is not widely utilized at VAMCs.

c) A report titled the "PRCNTEG" report can be run to compare the original "checksum" values of IFCAP version 5.0 to the "checksum" values at a VAMC. A "checksum" value is a specific number associated with the length of a file and is used to identify changes in that file or series of files. The "PRCNTEG" report will identify any "checksum" changes that do not match the original checksum of IFCAP 5.0 and can be used to monitor whether changes to IFCAP have been made. No formal periodic review of the "PRCNTEG" report is performed to ensure that local modifications have not been made to IFCAP systems running at the VAMCs.

The distribution of "programmer mode" access to IRM and ISC staff provides these users with the capability to modify IFCAP routines and data. Without appropriate monitoring procedures designed to ensure that the integrity of IFCAP routines and data is preserved, there is an increased risk that these files may be accessed and modified without management's approval.

Recommendation 9:

We recommend that:

a) Management review users with "programmer mode" access privileges for appropriateness and restrict this privilege to only those members of the IRM and ISC staff for which this capability is required for them to perform their job function.

b) Management implement formal monitoring controls over the use of "programmer mode" and monitoring controls to ensure the integrity of IFCAP routines and data is preserved.

Under Secretary for Health's Comments

We concur with clarification. On some occasions, access privileges are necessary for staff outside of IRM. In those instances, appropriate security clearances for "programmer mode" access privileges are required as stipulated in M-11, Chapter 16. MISS will assure that issues relating to review of programmer access privileges, associated documentation and review of audit trails be communicated to field facility staff via the communication tools described in other sections of this action plan.

Planned September 1996 and Ongoing

Abt Team's Response

Management's response satisfies the intent of our recommendation.

B. MANAGEMENT ADVISORIES

This section addresses issues which have been identified as Management Advisories and not as Audit Findings. These Advisories address areas outside the scope of this audit but which were identified during fieldwork of Phase III. Many of these Advisories are related to the recommendations outlined in *Subsection A, Findings and Recommendations.*

1. Improve The IFCAP Application Training Curriculum.

The VA employed a "Train the Trainer" approach for IFCAP Release 5.0 end-user training. A limited number of users from each VAMC attended national training on the use of IFCAP and were then responsible for training remaining users locally. Many users, however, indicated that IFCAP training was not sufficient to ensure competency in the use of application functions and control features.

For example, IFCAP training did not appear to address the IFCAP interface with the FMS system. Familiarity with the IFCAP application and its interface varied greatly between individual IFCAP users and collectively among VAMC field sites. In addition, it appears that minimal training was provided to management personnel to assist them in establishing control over the system and directing lower level staff in their use of the system.

In order to ensure that all IFCAP application users are appropriately trained and capable of performing necessary job requirements, we recommend that the VA ensure standardization and consistency of IFCAP application training. Standardized training should include both management and end-user courses designed to address both the application's functionality and the manual procedures surrounding its use.

2. Consider Establishing A Formal, National Function To Facilitate The Communication Of Known Problems, Work-Around Solutions To Problems, And Best Practices.

During the course of the implementation of IFCAP Release 5.0, a weekly national conference call was established among IFCAP users for the purpose of discussing issues associated with the new release. The conference call facilitated the informal communication of known problems, work around solutions devised for these problems, and recommended "best practices" by VAMCs which had implemented Release 5.0 prior to others.

While the conference call provided assistance to participants, it became evident that errors in the use of the system were being repeated among sites and that duplication of effort was being performed in some cases. For example, problems discussed and work-around solutions offered during one conference call were mentioned as having existed as early as alpha and beta site testing.

We recommend that a resource be established and tasked with identifying and communicating software implementation issues and best practices to VAMCs. Such a resource should ensure that information is shared among all VAMCs as timely and efficiently as possible.

3. Review IFCAP Reporting Capabilities To Ensure That Users Are Provided With The Information Necessary To Perform Their Job Function.

IFCAP provides several standard reports designed to assist various users of the system in the performance of their job function. We noted that VAMCs relied upon several "FileMan" routines to assist in the reporting and analysis of IFCAP transactions. Use of "FileMan" routines to create reports requires specific access privileges and knowledge that may vary among the various VAMCs. In addition, the demand for additional reports to be generated from IFCAP could also vary among VAMCs.

While the skill to generate additional IFCAP reports may vary among VAMCs, and the demand for additional IFCAP reports may also vary, the apparent need for additional IFCAP reports appears to be very consistent.

We recommend a periodic review of the current reporting capabilities within the IFCAP application be performed, and where appropriate, additional reporting capability be implemented. In the performance of such a review, the opportunity exists to identify "best practices" that may be performed at individual VAMCs that could be applied across all VAMCs.

4. Consider Requiring All VAMCs To Install Part 3 Of Kernel To Improve Security Over IFCAP Files.

The Kernel system is a component of the operating system environment in which IFCAP is executed. The Kernel provides utilities which facilitate DHCP functionality, including several security programs which provide access control over application data files. One security program, known as Part 3, is an option of the Kernel system which may be utilized by VAMCs to better secure these data files. When installed, access to files can be explicitly granted to each user, rather than being granted to all users sharing a common access code.

During our review, we observed that only one VAMC had installed Part 3 of Kernel. While management personnel at this VAMC stated that significant resources were necessary to specifically tailor user access to IFCAP data files based on each users' job responsibility, management also noted improved security over IFCAP data files and greater flexibility in administering security once Part 3 had been established

We recommend that the VA consider requiring all sites to implement Part 3 of the Kernel system to help ensure that appropriate security has been established over IFCAP data files.

5. Improve Testing Practices For IFCAP.

We noted that there were many programming errors with the release of IFCAP version 5.0. We reviewed a log maintained by the ISC of all the problems identified with the release of IFCAP 5.0 and noted that there were over 500 problems. Upon our review of this problem list, it was apparent that many of them could have been identified if proper testing were performed.

In order to ensure deployment of a quality application, adequate programmer and user testing needs to be performed to ensure all changes are accurate and meet the needs of the user community. When testing is not performed adequately, changes can be introduced into the system that can potentially corrupt data and negatively impact functionality.

We recommend that a review of current testing practices over the IFCAP application be performed to assess the effectiveness of current procedures. We also recommend that based upon this review, appropriate testing strategies be implemented to help minimize the risk of errors being introduced into the systems development process.

6. Remove Users' Ability To Edit Their Electronic Signature Block.

Currently, IFCAP users are permitted to alter their electronic signature block name. The changes that can be made to the electronic signature block are limited in that the system requires the user's last name "string" (i.e., "WILLIAMS" as in "John WILLIAMS") to appear in the block. However, users can modify/delete their block first name and middle initial while adding characters to the beginning or ending of the last name.

For example, a user may change their electronic block signature from "John WILLIAMS" to "Diane WILLIAMSon." As the electronic signature block represents the name that will be printed on documents evidencing authorization, changes to the signature block could allow users to print authorization documents with invalid system users' names.

In order to ensure that all documents evidence proper authorization, we recommend that users not have the ability to change their electronic signature code and that when a document is signed the system automatically assigns the user's name to their electronic signature block. This will ensure that all documents are signed with the name given to that approving user by security management.

SECTION III:

Overview of IFCAP and Related Controls

SECTION III: OVERVIEW OF IFCAP AND RELATED CONTROLS

In 1982, a Department of Veterans Affairs (VA) executive order established the Decentralized Hospital Computer Program (DHCP), and introduced the process of developing and maintaining internally a totally integrated medical center information system. This system is built around a local VAMC patient and administrative database and supports both local VAMC and agency wide management needs.

One of the applications which forms the DHCP is IFCAP, an application designed to support a variety of VAMC administrative activities. The general functions of IFCAP include funds distribution, funds control, expenditure requests, purchase orders, receiving, and inventory control. An overview of the significant functionality enhancements to IFCAP introduced in Releases 3.5, 4.0, and 5.0 is provided in *Subsection A* below.

IFCAP provides critical functionality to VAMCs. As a result, the integrity of information recorded and processed by IFCAP is of paramount importance to the VA. A complex system such as IFCAP involves numerous programmed procedures which cannot be checked in detail solely by the user, nor can they be controlled entirely through examining information output from the system. Rather, such a system is controlled, in large part, through application controls surrounding the use of IFCAP and IT controls over the operation of the system at each VAMC.

Strong application controls ensure that all transactions are approved and accurately posted to the system. Application controls related specifically to Phase I findings were reviewed and are presented in *Subsection B* below.

IT controls provide the VA with the assurance that the information processed by IFCAP is secure and has integrity, that the system and data is available when needed, and the functions of the application are consistent across each VAMC. For purposes of this audit, IT controls were categorized as System Security, Backup and Recovery, and Application Maintenance Controls. Descriptions of typical IT controls employed by the VAMCs are provided in *Subsections C, D*, and *E*, respectively.

A. FUNCTIONALITY OVERVIEW

Documented below are significant functional enhancements introduced within IFCAP Releases 3.5, 4.0, and 5.0. Functions are listed by IFCAP module. The IFCAP Release in which the function was introduced is identified in parentheses.

Funds Distribution Module

IFCAP provides the functionality to increase and decrease funding to a Fund Control Point (FCP) and to transfer funds between FCPs. These transactions are automatically posted from IFCAP to the FMS system. *(Release 5.0)*

Additionally, new rollover processing of fund balances from one quarter to another has been established. IFCAP may be configured so that a balance is automatically rolled over from one FCP to another as specified by the user; is automatically rolled over to the same FCP; or is automatically rolled over for all FCPs. *(Release 5.0)*

Control Point Module

Significant enhancements have been made to the Control Point Module. IFCAP now notifies Control Point Clerks of the number of requests awaiting processing. *(Release 4.0)* Additionally, processing of requests for expenditures (1358s) at the control point level includes several safeguards to ensure that authorizations and actual expenditures do not reduce the original obligation to less than zero without prompting the FCP to create an increase adjustment. *(Release 5.0)*

FCPs must be configured within the system to overcommit funds.   If overcommitting is not allowed for the FCP, IFCAP then checks the rollover fields for available funds from prior quarters as described above. *(Release 5.0)*

Procurement Module

When vendor information is added or updated within IFCAP, a vendor request document is sent to FMS. Once the vendor unit in Austin, TX confirms the accuracy of the addition or update to the vendor file, FMS transmits a vendor update document to update the IFCAP vendor file. Should the vendor unit make any changes to the vendor information in FMS, these changes would be updated in IFCAP via the vendor update document, thereby maintaining consistency of the vendor files between the two systems. *(Release 5.0)*

Enhancements have been made to the Purchase Order (PO) and Requisition Amendment process. Amendment/Adjustment voucher processing has been modified so that IFCAP documents do not change until Fiscal approves the changes. Amendments now automatically adjust FCP balances.

IFCAP no longer allows Amendments to POs or Requisitions with "transaction complete" status, with the exception of Certified Invoices. *(Release 5.0)*

Payment / Invoice Tracking Module

IFCAP creates and transmits Payment Voucher documents to FMS. The Payment Voucher document notifies FMS of Certified Invoices processed in IFCAP. A new Edit FMS Vendor Payment Information option allows the Voucher Audit Clerk to edit the name or payment information, or add new vendors to IFCAP upon receipt of certified invoices. Use of this option initiates a vendor request document to FMS to add/update vendor information in the system. *(Release 5.0)*

Cross-references from invoices to POs, vendors, and FCPs have been added to IFCAP. Specifically, the cross-referencing allows users to view other invoices for the purchase order, view other invoices entered for the same vendor, request a list of transaction numbers for a given FCP, and enter an FMS Payment Voucher document number. *(Release 5.0)*

General Inventory Package Module (GIP)

The warehouse, primary, and secondary inventory points automatically calculate and set the stock levels and reorder points in IFCAP. The stock levels and reorder points are calculated as a percentage of the average usage during a specified period. The user may enter the percentage to use when calculating the stock levels and reorder points. *(Release 5.0)*

Barcode capability for data acquisition has been implemented at the inventory point using a portable bar-code reader to enhance inventory accuracy, reduce data entry errors, and reduce the time that it takes to complete an inventory. *(Release 3.5)*

Accounting Module

The Accounting Module of IFCAP was significantly enhanced to interface with the FMS system. The following IFCAP transactions are automatically uploaded to FMS *(Release 5.0)*:

a) Upon initial obligation of a Purchase Order (PO), IFCAP creates and transmits the FMS Miscellaneous Order (MO) document.

b) Upon obligation of an Amendment to a PO, IFCAP creates and transmits the FMS modification entry.

c) Upon initial obligation of a 1358 or a Certified PO, IFCAP creates and transmits the FMS Service Order (SO) document.

d) Upon obligation of a 1358 Adjustment, IFCAP creates the FMS modification entry SO.

e) Upon obligation of an Amendment to a Certified PO, IFCAP creates the FMS modification entry SO document.

f) Upon approval of a Receiving Report, IFCAP creates a Receiving Report Record and sends the record to the IFCAP Federal Receiving Report System.

IFCAP and FMS transactions are passed from one system to another daily. All FCP transactions originating in IFCAP are shown in the Running Balances Report (replaces the 820 report from the CALM system). All FCP transactions not originating in IFCAP (i.e., originating in FMS; for example, late receipt of goods resulting in interest expense) are shown in the FMS Transaction Data Report. *(Release 5.0)*

The Stack File records the FMS Document transmission information and contains MailMan message data, data processing center confirmation data, and status information. Users may manually create, edit, and delete FMS documents (transactions) that IFCAP does not create automatically using IFCAP's FMS Code Sheet Menu. Additionally, users may purge transmitted and confirmed documents, re-transmit stack file documents (for which no confirmation has been received), and print the status of selected stack documents. *(Release 5.0)*

Purchase Orders, receiving reports, and 1358s contain information captured in a file as each document is processed which can be printed at a later date and time. This information includes the internal entry number of the record, the date the document was created, and the external record number of the document. *(Release 4.0)*

B. APPLICATION CONTROL PROCEDURES

Application controls are procedures directed at achieving certain control objectives for transactions or events of an enterprise. Some of these controls are performed manually; for example, the manual reconciliation of control point fund balances between the IFCAP and FMS systems. Other controls are carried out by the IFCAP application; for example, the automatic matching of a receiving report with a purchase order. Many application controls will be performed by people but will be computer dependent, that is, a combination of programmed control procedures and user controls. An example is the review of a purchase request by a Control Point Official and the Official's approval through an electronic signature recorded in the system.

As described in Section I of this report, application control objectives as they relate to Phase I findings were reviewed. These control objectives included:

a) *Separation of duties*

b) *Identification of duplicate transactions*

c) *Purchase order approvals*

d) *Outstanding transactions and exceptions*

e) *Supervisory controls*
f) *Supervisory review over receiving transactions and inventory exceptions*
g) *Periodic review of override exceptions*
h) *Review of actions taken to resolve errors and exceptions*

Separation of duties

Separation of duties within an application ensure that users are precluded from initiating, recording, reviewing, and approving the same transaction. Within IFCAP, transactions entered into the system are required to be electronically signed by an appropriate official before being sent for further processing within the system. Typically, requests for expenditures and purchase order requests are initiated within the IFCAP system by an established IFCAP control point requester. Control point requests are processed and established as a permanent IFCAP request when a transaction number is assigned within IFCAP by the Control Point Clerk. Permanent requests are then approved by an authorized control point official and are automatically placed within an electronic purchase order for review by a purchasing agent within the Acquisition & Materials Management Service (A&MMS).

Once reviewed and processed by a purchasing agent, purchase orders are released for further processing and obligation within the Fiscal Service. Accounting Technicians within Fiscal Service are responsible for obligating control point funds to fulfill the pending purchase orders (2237s) or requests for expenditures (1358s).

Typically, control point funds distribution is performed by the Budget Analyst within the Fiscal Service. Upon manual approval by the Fiscal Service Chief, each control point fund balance is updated by the Budget Analyst using the funds distribution function within IFCAP. Control point budgets are generally updated on a quarterly basis.

Identification of duplicate transactions

Application controls should exist to detect and prevent duplicate transactions from being posted within the IFCAP application. Within IFCAP, each transaction entered into the system is automatically assigned a sequential tracking number. The IFCAP system alerts users of transactions which have already been processed through the system. However, the IFCAP system will accept duplicate requests if entered as separate and unique transactions. VAMCs rely upon manual user procedures to prevent the processing of duplicate transactions.

Purchase order approvals

Purchase order requests should be reviewed and approved by an appropriate individual prior to release to the next processing stage. IFCAP does not require the complete review of 2237s or

1358s by the Control Point Official prior to approval. Upon logon, Control Point Officials are automatically prompted as to the number of requests awaiting their approval. Summary information for each transaction is displayed by the system at the time that the Control Point Official grants approval through an electronic signature recorded in the system. Each request is summarized to include the requesting control point, transaction number, item description, and dollar amount of the item requested. The review performed by Control Point Officials is designed to ensure that the request is appropriate, and that dollar amounts are reasonable and within funding limits.

Control Point Officials are given the option within the system to review the complete transaction on-line prior to approval. This procedure however is not required in order for a request to be approved.

Outstanding transactions and exceptions

Reporting of outstanding and exception transactions helps ensure the timeliness and efficiency of processing. In addition, the use of these reports to account for transactions ensures the completeness of transaction processing.

IFCAP users monitor the status of 2237 and 1358 requests on-line using the Transaction Status Report. The Transaction Status Report lists transactions by number and details the purchase order number, the dollar amount of the request, and the current status within the IFCAP system. However, no system control is currently in place requiring VAMC personnel to review the Transaction Status Report on a routine basis.

All IFCAP transactions which have been processed and sent to FMS are detailed within the daily IFCAP Acceptance Listing. The IFCAP Acceptance Listing details each transaction accepted by the FMS system for the previous day. This listing provides personnel within the Fiscal Service with the ability to review and monitor transactions entered and successfully processed within the IFCAP system.

IFCAP transactions which were rejected by the FMS system are detailed in the FMS Rejection Listing Report. The Rejection Listing Report details the specific transaction number of the item rejected and the reason why the transaction was rejected by the FMS system. Each rejection must be corrected and resubmitted for acceptance by the FMS system. Typically, the Rejection Listing Report is reviewed by Fiscal Service on a daily basis and initialed and dated as reprocessed by the responsible Accounting Technician.

The Data Processing Center in Austin, Texas notifies VAMC purchasing agents (via system messages) of electronic data interchange (EDI) transactions which were rejected by the vendor. The purchasing agents are then responsible for resolving and investigating EDI rejections with the vendor and resubmitting the purchase order.

Supervisory controls

Supervisory controls ensure that supervisory control procedures are established and enforced over transaction processing. These control procedures help to ensure that transaction processing is performed appropriately and that supervisory review over transaction processing is conducted in a timely manner.

Fiscal Service personnel review the FMS Status of Funds Report which details each control point's fund balance and current obligation to monitor the level of activity and dollar amount of 2237 and 1358 requests being processed within each control point. In addition, daily transaction Acceptance Listings, Rejection Listings, and Activity Summary Reports are produced and available for review as needed. Finally, Fiscal Service and A&MMS Chiefs review Transaction Status Reports to monitor the status of each request within the IFCAP system.

Supervisory review over receiving transactions and inventory exceptions

Warehouse personnel review the respective purchase order on-line and examine the description of items ordered to ensure the goods received are in agreement. Goods received not having a related purchase order within the IFCAP system cannot be posted within the system prior to the release of an approved purchase order from Fiscal Service. Before releasing received goods to the requesting service, the individual requester is required to sign the receiving report to indicate the receipt of goods. Upon delivery and acceptance of goods received, the receiving report and packing slip are typically delivered to the A&MMS Warehouse Manager for review and then filed within the Materials Management Division.

The current IFCAP application does not allow for receipt overages to be posted against the original purchase order transaction. An amendment to the purchase order transaction must be processed and approved, or overages must be returned to the vendor.

Inventory counts are taken semi-annually, with spot checks of inventory levels conducted on a periodic basis by A&MMS personnel. IFCAP provides inventory count worksheets which are used by warehouse personnel to verify inventory levels. Differences are noted and recorded within the Inventory Adjustment Summary Worksheet. Typically, errors are first recounted and then posted within the system as an adjustment to inventory.

Periodic review of override exceptions

Purchase requests are reviewed, approved, and processed by purchasing agents. Override of goods requested or the consolidation of two or more purchase orders is performed by the purchasing agents at their discretion. Generally, notification is sent to both the requesting official and the Purchasing Chief through a phone conversation or electronic mail message. These events, however, are not specifically required to be reviewed by senior management. Monitoring of these events by supervisory personnel is conducted through daily feedback, examination of on-line status reports, and observation.

Expenditure amounts are limited to fund balance by control point. Control points may overcommit funds if approved by the Fiscal Chief and so designated within the IFCAP application. As with requests within approved funding levels, purchase orders and requests for expenditures which overcommit a control point must also be approved by Fiscal Service. In addition, total expenditures and fund balance by control point and by station are monitored through the FMS Status of Funds Report.

Review of actions taken to resolve errors and exceptions

IFCAP transactions which are not accepted by the FMS system are identified and reported daily within the FMS Rejection Listing Report. Accounting Technicians are generally responsible for correcting and reprocessing IFCAP rejections. Corrections to the rejection listing are typically documented and filed within Fiscal Service. Rejections requiring multiple submission attempts or resolution are typically submitted to the Fiscal Chief for review. In addition, various reconciliations are performed by the Control Points and/or Fiscal Service to monitor available funds and ensure that all transactions are processed accurately.

C. SYSTEM SECURITY CONTROL PROCEDURES

System security controls are implemented over the operating system, application programs, and data files of an information systems environment. The objective of system security control procedures is to provide assurance that the operating system and application programs and data files are protected from unauthorized access.

During the review, we focused on the following system security controls at each VAMC:

a) *Security Management*
b) *System Level Access Controls*
c) *Application Level Access Controls*
d) *Access Controls To Sensitive Facilities*
e) *Physical Access*

Security Management

Security management controls help to ensure that appropriate security awareness exists, that access control policies have been implemented, and that a secure computer environment is maintained. Typically, the Chief of A&MMS and Chief of Fiscal Service are assigned ownership of IFCAP data. Each user's Service Chief is responsible for assigning access to menus, options, and security keys within their applications. Information Resource Management Service (IRMS) personnel are assigned the responsibility of performing security administration activities.

VAMCs typically maintain a Security Policy and Guidelines which provides guidance on general security administration procedures and the roles and responsibilities of designated security administration personnel. The document typically includes guidelines for access controls over various applications, networking and telecommunications, sensitive data, physical security, and security monitoring of VAMC personnel.

Upon receiving their access code to the system, new users are generally required to read and electronically sign an Access Agreement form prior to establishing the verify code needed to gain system access.

System Level Access Controls

System level access controls help to ensure that access to the operating systems, programs, and data are appropriately restricted. The operating system at most VAMCs is the DEC VAX/VMS system. VMS user-IDs and passwords are assigned by IRMS and are typically for use by IRMS personnel to maintain the information systems environment.

Programmers within IRMS are responsible for maintaining and operating the IFCAP application. These individuals usually have read/write access to IFCAP's application programs and data files through "Programmer Mode" in the Kernel application. However, logging and review of programmers' activity is not generally performed. In addition, programmers also have read/write access to IFCAP data through the VA FileMan utility. Use of this utility is also not generally logged or reviewed.

As noted above, Service Chiefs are responsible for requesting IFCAP access for users by completing a User Access Request Form. Service Chiefs are additionally responsible for specifying the menus, options, and security keys to be granted to the user and ensuring that the access granted is commensurate with the users' responsibilities. IRMS establish, delete and modify user access privileges to the Kernel and IFCAP application as detailed on the approved User Access Request form, and assign the Access and Verify codes.

The IRMS receives notice from Service Chiefs if user access requires modification to reflect changes in the user's responsibilities. Additionally, Human Resources Service typically forwards the Gains and Losses Report at least monthly to IRMS. The report details new users, terminated users, and users whose responsibilities have changed. IRMS uses this list to update system access accordingly and to ensure that access remains commensurate with job responsibility.

IFCAP utilizes Electronic Signature Codes to facilitate IFCAP's "paperless" processing functions. The Electronic Signature Code helps to authenticate the user's authority to perform certain transactions such as: approving requests, releasing funds, obligating documents, establishing receivables, processing orders, authorizing payments, and receiving purchases. Users with

Electronic Signature codes have the ability to change their own Signature code at any time. In addition, users are permitted to edit their Electronic Signature Block first name, however the Kernel prohibits the deletion of the user's (block) last name.

When a user attempts to electronically sign a document, the system verifies that the person currently logged onto the system is the same person who is trying to electronically sign the document. The system accomplishes this task by passing the Electronic Signature code entered by the user through a hashing algorithm and comparing the hashing total to the total maintained in the user file of the person currently logged into the system. A match indicates that, unless a user has shared their Electronic Signature code with another person, the person entering the code is the authorized user.

Application Level Access Controls

Application level access controls ensure that access to particular functions within an application are appropriately restricted to ensure segregation of duties and prevent unauthorized activities. Security within the IFCAP application is maintained through the use of IFCAP menu options and security keys. To use IFCAP, users must possess access to both the appropriate menus and have the necessary security keys. Both menus and keys are defined in the user's profile in the Kernel system. Additionally, control point requesters, clerks, and officials must be defined as a control point user for a particular control point in the IFCAP file 420 (Control Point Fund).

Access Controls To Sensitive Facilities

Access to sensitive facilities such as master passwords, powerful utilities, and system manager facilities should be appropriately restricted and monitored. System users with the ability to enter Programmer Mode have virtually unrestricted access to all DHCP applications and data, including IFCAP. Generally, only personnel within IRMS and the Information Systems Center (ISC) have the ability to enter into the programmer mode. The Kernel system can be enabled to log users who enter into programmer mode.

The capability to directly edit IFCAP data files through VA FileMan is generally restricted to a limited number of IRMS staff and ISC users. In addition, IRMS personnel have the ability to create local security keys which can perform the same functions as the national keys, as well as other functions.

Physical access

Physical access to computer facilities and data should be appropriately restricted. Typically, DHCP servers and other communications equipment are physically secured in the VAMC's data center. Access to the data center is generally limited to IRMS and is secured through the use of card keys or similar physical protection devices.

D. BACKUP AND RECOVERY CONTROL PROCEDURES

The objectives of backup and recovery control procedures are to provide assurance regarding the restoration of computing capabilities and facilities after a system failure. The following computer operation controls, as they relate to the operation of IFCAP at a VAMC, were reviewed:

a) *Backup*
b) *Recovery from Operational Failures*

Backup

Up-to-date backups of programs and data should be available to minimize the impact of data corruption, operational downtime, or emergencies. Typically, a full system backup is performed weekly and an incremental backup is performed nightly. The backup procedure is generally executed automatically by the system. Backup tapes are typically stored in a locked file cabinet located within an area of the VAMC separate from the data center. Tapes are rotated off-site on a weekly basis.

In addition, VAMCs typically utilize a separate file server(s) to shadow the live data file servers. When shadowed, transactions are stored in both the live and the shadowed file server to maintain redundancy within the system.

Recovery from Operational Failures

Appropriate procedures should be in place to ensure that operational failures are identified, resolved in a timely manner, and approved retrospectively by the appropriate staff and users. Most VAMCs have drafted a Disaster and Contingency Plan; however, the plan has not typically been completed or tested.

E. APPLICATION MAINTENANCE CONTROL PROCEDURES

Application maintenance controls provide assurance that program changes are properly approved, tested, and implemented. The following application maintenance control objectives were reviewed at each VAMC:

a) *Application Monitoring*
b) *Application Configuration*
c) *Requests for Application Changes*
d) *Testing of Application Changes*
e) *Transfer of Application Modifications into the Live Systems Environment*
f) *User Documentation and Training*
g) *Patch Documentation*

Application Monitoring

Application monitoring controls help to ensure that the application is performing as designed and is fulfilling users' requirements. Generally, user needs and views regarding functionality and operational quality are informally communicated to IRMS through memos, phone conversations, or electronic mail messages. IRMS may also meet with Automated Data Processing Application Coordinators (ADPACs) to gain an understanding of problems with the application and potential enhancements. In addition, users may formally communicate views, concerns, or other issues through the Electronic Error & Enhancement Reports forum (E3R). Problems identified with IFCAP releases are communicated to the ISC via a NOIS (National On-line Information System) document.

Application Configuration

IFCAP has many options and parameters which alter the way in which it operates at each installation. For example, IFCAP may be configured to accept or not accept receipt overages, depending upon the parameter chosen for that configuration option. Significant configuration options should be appropriately controlled to ensure that they do not adversely affect the controls built into the system.

IFCAP Application Coordinators (ADPACs) are responsible for maintaining system site parameters via configuration options through IFCAP menus. Access to these menus is restricted by Service Chiefs who are responsible for ensuring that access to the system is appropriate. The configuration options are established based upon input from IRM, ISC, and the Application Coordinators.

Requests for Application Changes

User requests for changes to IFCAP should be appropriately considered, approved, prioritized, and monitored. As noted above, user requests for local modifications are communicated informally to IRMS personnel and ADPACs. Requests for significant changes to IFCAP are communicated to user groups and the ISC through the use of E3Rs and NOIS messages. Few local modifications may be made to IFCAP under the Veterans Affairs Health Administration

(VHA) Directive 10-93-142 and modifications are generally limited to informational reports as requested by VAMC system users.

Testing of Application Changes

Appropriate testing of application changes should be performed to ensure that changes will not adversely impact the overall functionality of the application and that changes meet user requirements. VAMCs typically establish a test environment for use in training and testing of local modifications and enhancements. Generally, minimal testing is performed for verified IFCAP releases and patches.

Transfer of Application Modifications into the Live Systems Environment

The implementation of changes to the live environment should be controlled to ensure that all changes are tested and approved prior to implementation. Typically, informal controls exist to ensure that only properly tested, reviewed, and approved changes are transferred into the live environment. VAMCs rely upon security controls to ensure that only authorized individuals have update access to the live environment. These individuals are typically IRMS personnel. However, reviews of the live environment to detect unauthorized changes are typically not performed.

User Documentation and Training

Users should be appropriately trained as new releases of IFCAP are distributed to ensure the proper use of the application and to ensure that the application is utilized to its fullest extent. In addition, users should receive appropriate documentation to serve as reference or guidance material as they perform their job responsibilities.

Training on the IFCAP application is conducted through a "Train the Trainer" approach. Selected individuals receive training at a national level; these users are, in turn, responsible for conducting training at their local VAMC. In addition, IRMS and ADPAC personnel often serve as application experts and can assist new users when necessary.

The IFCAP application is accompanied by Technical and User Manuals as well. These manuals typically reside in the IRMS and ADPAC offices; however, selected portions of this material may also be located with users as needed.

Patch Documentation

Patches to the IFCAP application should be appropriately documented. In addition, this documentation should be made available to IFCAP users to ensure that they are aware of changes in functionality or controls which may impact the performance of their job functions.

Patch documentation is made available to all VAMCs when changes to IFCAP programs are distributed. Typically, IRMS personnel or ADPACs assess the impact of patches on IFCAP functionality. Users may review patch documentation; however, knowledge of changes to functionality and controls is communicated verbally by IRMS and the ADPACs.

APPENDIX A:

Audit Issues Matrix

Audit Issues Matrix

Audit Issues	Site						
	1	2	3	4	5	6	7
1. Ensure That Appropriate Separation Of Duties Is Achieved Over The Initiating, Recording, Reviewing, And Approving Of IFCAP Transactions.							
• Certain IFCAP users have access to the application which generally is granted to users in other services and which appears to represent conflicts of interest, including:							
• The Fiscal Accountant maintains IFCAP menu access for Control Point Official, Accounting Technician, and Funds Distribution. In addition, the Fiscal Accountant possesses system security keys normally granted to the Fiscal Chief.			✓				
• The Fiscal Chief possesses access to assign A&MMS menus and security keys to IFCAP users.			✓				
• A Management Analyst within Fiscal Service possesses access to both purchase and obligate authority.							✓
2. Strengthen Operating System Security Controls.							
• Kernel site parameter settings vary from recommended settings included in the Kernel systems documentation and industry standards. These settings include: • Failed access attempts are not logged. • Number of invalid logins permitted prior to the system disabling the user's device is excessive. • Multiple logins for users (not including those users directly responsible for delivering patient care) are allowed. • Verify Code lifetimes are greater than 90 days.	✓	✓	✓	✓	✓	✓	✓
• User accounts have been identified at the VMS system level that have minimum password lengths less than six characters	✓	✓					✓
• User accounts at the VMS level have obvious passwords (i.e. passwords that audit software for the VMS environment was able to guess).	✓			✓	✓	✓	✓
• User accounts were noted to have unlimited password lifetimes. (i.e. the system does not require the user to change their password)	✓	✓		✓	✓		✓

Audit Issues	**Site**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
• User accounts had password expiration dates that exceeded the standard setting. (30 days for privileged accounts, 90 days for non-privileged)	✓	✓		✓			✓
• Accounts within VMS have been dis-usered which means they are no longer in use. These accounts should be removed from the system.	✓	✓		✓	✓	✓	
• User accounts have been identified that have duplicate UICs. (A UIC identifies a specific account. If two users have the same UIC management cannot monitor the activity of a particular account)	✓	✓		✓	✓	✓	✓
3. **Improve Security Administration Procedures.**							
• In general, we noted that a comprehensive periodic review of user access privileges is not performed.	✓	✓	✓	✓	✓		✓
• We noted that documentation is not consistently maintained for requests for primary and secondary menu options. Auditability of user access is significantly limited when documentation of access approvals is not maintained.			✓	✓	✓		✓
• We noted that the sites do not adequately document the distribution of additional primary and secondary menu options after a user has received system level access to DHCP.	✓	✓	✓	✓	✓	✓	✓
4. Improve VAMC Backup, Recovery, And Contingency Planning Procedures.							
• Daily incremental backups are not performed.		✓	✓		✓		
• Verification of backup tapes is not performed.		✓		✓			
• Disaster Recovery and Contingency Plan has not been fully completed nor fully tested.	✓	✓	✓	✓	✓	✓	✓
5. Improve The Reconciliation Procedures Surrounding The IFCAP And FMS Interface To Ensure Timely Reconciliations.							
• The reconciliation of control point fund balance between the IFCAP and FMS systems requires significant effort due to budget, timing, and other differences between the two systems. Reconciliation procedures varies among sites. Many control point personnel stated that they are typically unsure as to the available funds balance for a control point.				✓	✓	✓	✓

Audit Issues	**Site**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
6. Strengthen Controls Surrounding The Use Of IFCAP To Ensure That Specific IFCAP Transactions Are Authorized, And Processed Completely And Accurately.							
• Inventory count personnel are provided with system generated on-hand inventory totals prior to conducting each inventory inspection.				✓	✓	✓	
• Inventory adjustments are posted prior to review and approval of the "Adjustment Approval Form" by management personnel.			✓	✓	✓	✓	✓
• Typically, various documents automatically print within the Fiscal and A&MM Services when they are ready for processing. However, should a printer be unavailable at the time a documented is forwarded to Fiscal Service or A&MMS, and remain unavailable for an extended period of time, these documents become "lost" within the system and are not processed until they are individually identified as outstanding.		✓	✓	✓	✓	✓	✓
• Purchasing agents authorize and obligate purchase order requests for the General Supply Fund control point without Fiscal service approval.				✓	✓	✓	
• Goods received prior to the obligation of a purchase order may not be recorded within the IFCAP application. We recommend that goods received prior to the obligation of a purchase order be recorded in IFCAP in a suspense file to ensure that record of their receipt is maintained.			✓	✓	✓	✓	✓
7. Document The Purpose And Assignment Of Locally Developed IFCAP Menu Options And Security Keys.							
• VAMC sites have created local security keys which are used as "locks" or "reverse locks" on specific menu options. When used as reverse locks a key may allow access to options that could have security implications. These security keys and their purpose, as well as to whom they have been assigned, are not always documented by IRM.	✓			✓	✓		✓
• Locally developed menus are created by IRM or ADPACs to tailor IFCAP menu options for specific users. No formal documentation identifying the purpose and functionality of these menus is maintained for auditability. In addition, the distribution of these menus is also not documented.	✓			✓	✓		✓

Audit Issues	Site						
	1	2	3	4	5	6	7
8. Strengthen Controls Surrounding The Assignment And Monitoring Of FileMan Access To IFCAP Data Files.							
• The IFCAP Security Guide recommends FileMan access settings over key IFCAP data files to help ensure data integrity. Several VAMCs have changed the FileMan access settings over IFCAP files.	✓	✓		✓	✓		✓
• Monitoring of FileMan access and use is not formally performed or required by the VAMC hospital.	✓		✓	✓			✓
9. Improve Access Controls And Monitoring Procedures Surrounding Programmer Access To IFCAP.							
• All IRM staff with programmer mode access have update access to the IFCAP production environment. This includes staff not responsible for maintaining the IFCAP application.	✓	✓	✓	✓	✓	✓	✓
• At various sites the ability to enter into programmer mode has been granted to IRM staff as well as members of the ISC from remote locations. The system does allow for the logging of users who enter programmer mode however several sites do not formally review this log. In addition IRM staff have the ability to bypass the logging feature which may limit the completeness of the log.	✓	✓	✓	✓	✓		✓
• Formal change control procedures do not exist over the production environment. In addition, review of the production environment for unauthorized code is not performed.	✓	✓	✓	✓	✓	✓	✓

Management Advisories Matrix

Management Advisories	Site						
	1	2	3	4	5	6	7
1. Improve The IFCAP Application Training Curriculum.							
• Standardized system training was not provided to all IFCAP users. It was communicated that a limited number of users from each VAMC attended national training on the use of IFCAP and were responsible for training remaining users in a "Train the Trainer" approach. However, many users indicated that IFCAP training was not sufficient to ensure competency in the use of application functions and control features.				✓	✓	✓	✓
• No management-level training or update on changes in functionality was provided to management personnel.				✓	✓		✓
2. Consider Establishing A Formal, National Function To Facilitate The Communication Of Known Problems, Work-Around Solutions To Problems, And Best Practices.							
• No formal, national function appears to exist to communicate to VAMCs known problems previously encountered by other VAMCs, work-around solutions to those problems, and best practices.				✓	✓	✓	✓
3. Review IFCAP Reporting Capabilities To Ensure That Users Are Provided With The Information Necessary To Perform Job Function.							
• Numerous FileMan reports have been developed to address specific information needs at VAMCs. Some of these reports appear to be significant in nature.					✓	✓	✓
4. Consider Requiring All VAMCs To Install Part 3 Of Kernel To Improve Security Over IFCAP Files.							
• Management should consider implementing the Part 3 option of the Kernel system to improve security over IFCAP files. When installed, access to files can be explicitly granted to each FileMan user, rather than being granted to all users sharing a common access code.	✓	✓	✓	✓	✓		✓

Management Advisories	Site						
	1	2	3	4	5	6	7
5. Improve Testing Practices For IFCAP.							
• VAMCs reported large numbers of problems with the release of FMS, IFCAP Release 5.0, and their interface. In addition, FMS Issues List, which lists bugs, operational issues, and enhancement for FMS, IFCAP, and their interface, numbered as high as 582 items at one point. It appears that better testing should be performed during the verification process of new releases to identify and correct problems with functionality prior to national distribution.	✓	✓	✓	✓	✓		✓
6. Remove Users' Ability To Edit Their Electronic Signature Block.							
• Although the Kernel does not allow a user to change the electronic signature block last name, a user can modify/delete the block first name and middle initial while adding characters to the beginning or ending of the last name. Thus the user could appear to sign documents with other names. For example 'John Williams' could become '**Diane** Williams**on**'	✓	✓	✓	✓	✓	✓	✓

Department of Veterans Affairs **Memorandum**

Date:

From: Under Secretary for Health (10/105E)

Subj: OIG Draft Report: ***Audit of the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) System, Phase III***

To: Assistant Inspector General for Auditing (52)

1. This report has been reviewed by involved program offices and we are pleased to note that the IFCAP system is performing as designed and that most internal controls at the facilities are operating satisfactorily. With one exception, there is concurrence in the findings and recommendations that pertain specifically to Veterans Health Administration. Concurrence is deferred on recommendation 2, pending more detailed review by advisory bodies within the Headquarters Office of the Chief Information Officer. As you have acknowledged in the cover memorandum accompanying this report, recommendations 5 and 6 should be more appropriately addressed by another Departmental program office, and we defer to the Deputy Assistant Secretary for Information Resources Management (045) in these responses.

2. As detailed in the accompanying action plan, the Medical Information Security Service (MISS), in conjunction with recently appointed Chief Information Officers (CIO) in the new VISN offices, is making concerted efforts to assure that field facilities are in full compliance with all phases of system security requirements. Regional training workshops for field staff, which will emphasize most of the security concerns addressed in this report, are scheduled for completion during the months of August and September 1996. MISS also administers periodic site visits to all facilities by the regional information security officers and conducts monthly national teleconference calls that involve participation by information system staff from all field facilities. Facility managers will be thoroughly briefed about findings in your audit and monitoring processes at the VISN level will be strengthened to assure that security procedures are fully enforced. VHA Headquarters staff will also work in

Page 2 OIG Draft Report: **Audit of the IFCAP System, Phase III**

close coordination with other Departmental offices to design and implement formal policy directives as needs are identified.

3. If additional information is required, please contact Paul C. Gibert, Jr., Director, Management Review Service (105E), at 273.8355.

Kenneth W. Kizer, M.D., M.P.H.

Attachment

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: OIG Draft Report: ***Audit of the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) System, Phase 111***
Report Number: Contract No. V101 (93) P-1201
Date of Report: none

Recommendations/ Actions	Status	Completion Date

RECOMMENDATIONS

1. We recommend that:

a) Management periodically review user access within IFCAP to ensure that the duties of initiating, recording, reviewing, and approving transactions may not be performed by the same individuals and,

b) Appropriate monitoring control procedures be established in those instances where conflicts of interest may not be avoided to prevent and/or detect unauthorized transactions from being processed within the system.

<u>Concur</u>

Representatives from the Offices of the Chief Information Officer (19), Chief Financial Officer (17) and Chief Network Officer (10N) will participate with the Office of Information Management (045) in assessing if a formal directive is required to address conflict of interest issues in the IFCAP application. If a directive is issued, procedures regarding security controls will be included. In the meantime, facility management will be apprised of the findings and recommendations of this audit that relate to identified security problems. These items will be included on the agendas of selected conference calls to the field conducted by Headquarters program offices and the VISN offices.

	Planned	December 1996

2. We recommend that the following enhancements be made to the VMS and Kernel systems' security configuration:

a) Log failed access attempts and ensure management review.

Page 2 IFCAP action plan

b) Disable devices after three to five invalid logon attempts.
c) Restrict multiple logons from users not directly responsible for delivering patient care.
d) Require verify codes to be changed every ninety days within the Kernel system.
e) Require minimum password lengths of at least six characters for VMS accounts.
f) Prevent and/or discourage VMS users from selecting obvious passwords.
g) Remove VMS accounts once dis-usered for more than thirty days.
h) Restrict VMS accounts from sharing user identification codes (UIC's)

Defer Concurrence

All of these systems' enhancements cannot be approved until they are jointly assessed and agreed upon by the Field Information Resources Management Advisory Council (FIRMAC), the Kernel Development Team, the Medical Information Security Service (MISS) and IRMFO Customer Support. The Chief Information Officer (CIO) will take appropriate steps to assure that these groups review OIG's recommendations for system enhancement and provide feedback about implementation feasibility. Based on evident justification for the individual enhancements, the CIO will assure that necessary corrective actions are taken.

Planned December 1996

3. We recommend the following improvements to VAMC security administration procedures:

a) Documentation of requests for, and approval of, user access to the IFCAP system be maintained to support the review and authorization of all user access.
b) Documentation of approval of all subsequent requests for approval be maintained.
c) Periodic review and approval of user access to ensure that access remains commensurate with job responsibilities.

Concur

The Medical Information Security Service (MISS) has provided sound policies, guidelines and suggested practices governing user access to VHA systems and data

Page 3 IFCAP Action Plan

that fully meet the intent of this recommendation. Numerous efforts are being made at the Headquarters level to encourage full compliance by the facilities with these directives. MISS is working closely with the VISN CIOs in coordinating informational exchanges with the field. For example, MISS will conduct three regional training workshops for information security officers (ISO) responsible for system security maintenance in the field facilities. Issues raised in this OIG report will be highlighted during these workshops, which will be conducted during the months of August and September, 1996. In addition, the MISS conducts monthly national conference calls, which include participation by all facilities. During the August 19 conference call, OIG's security administration recommendations will be reviewed and discussed and additional discussion will be included on the agendas of other conference calls as required. It is noted that minutes of the conference calls are routinely circulated to all facilities, thereby reinforcing discussed issues.

Planned Sept. 1996 and Ongoing

4. In order to provide assurance that system operations and data may be resumed in an efficient and timely manner in the event of operational failure, we recommend the development of standards governing system backups and data recoverability, and the implementation of these standards at all VAMCs. These requirements should include the appropriate nature and frequency of system backups, the periodic verification of backup tapes for integrity, and the periodic testing of disaster recovery and contingency plan procedures.

Concur

Appropriate policies, guidelines and suggested practices have been issued by MISS to field facilities regarding the development and testing of contingency plans. MISS is closely monitoring facility compliance with all aspects of contingency plan implementation and has recently developed an action plan which will bring all facilities into compliance with contingency plan requirements. A survey of all facilities has been completed by the Regional ISOs (as part of their regularly scheduled site visits) to determine levels of compliance with the contingency plan requirements. Survey findings and follow-up actions are being centrally tracked at the National Center for Information Security, and in coordination with the VISN CIOs, monitoring will continue until full compliance by all facilities is realized. An automated

Page 4 IFCAP Action Plan

contingency planning product that will facilitate the development and updating of contingency plans system-wide is also being considered for purchase , pending adequate funding support. MISS has also discussed the use of VA's Management Studies and Analyses contract with a vendor who can provide supplemental information security services in support of a national contingency plan development, testing and alternate site strategy. Again, approval of such a contract is dependent upon available funding.

Planned September 1996 and Ongoing

5. In order to ensure reconciliations for IFCAP and FMS interfaced transactions are being performed on a routine basis and in a timely manner, we recommend a review of current reconciliation procedures and the implementation of appropriate monitoring controls to reconciliation procedures and the implementation of appropriate monitoring controls to ensure the timely and efficient performance of reconciliations.

Defer action plan comments to the Deputy Assistant Secretary for Information Resources Management

6. In order that management may gain additional assurance that all IFCAP transactions are authorized and processed completely and accurately, we recommend the following:

a) A review of the controls over processing of "Inventory Adjustment Forms" should be performed to determine the importance to the VA of approving inventory adjustments prior to being posted in IFCAP. If it is determined that approval of inventory adjustments prior to update in IFCAP is important, we recommend IFCAP be modified to require an automated review of these forms prior to update.
b) Inventory totals in IFCAP should be removed from the "Warehouse Inventory Count Form" used by personnel performing physical inventory inspections.
c) A review of the controls over General Supply Fund transaction processing should be performed to determine the importance to the VA of having Fiscal Service review these transactions. If it is determined that Fiscal Service approval of General Supply

Fund transactions is desired, we recommend IFCAP be modified to require a review of these transactions prior to update.
d) An internal suspense file for the logging of goods received prior to fiscal obligation should be created in IFCAP to ensure that appropriate records of all received goods are maintained.

Defer action plan comments to the Deputy Assistant Secretary for Information Resources Management

7. In order to ensure that locally created security keys and menu options do not introduce weaknesses in the internal controls over IFCAP processing, we recommend VAMC management document and periodically review all locally developed security keys and menu options. In performing this process, VAMC management should place additional emphasis on controlling assignment of those security keys and options with powerful privilege within IFCAP.

Concur

This issue will be reinforced during the scheduled regional training workshops that were previously alluded to in this action plan. In addition, MISS will place special emphasis on issues identified in this recommendation during the routinely-conducted facility security site visits that are conducted by the Regional ISOs as well as during the monthly conference calls that are conducted by MISS.

Planned	September 1996 and Ongoing

8.. In order to ensure the integrity of IFCAP data, we recommend that:

a) Management periodically review FileMan access settings to IFCAP data files.
b) Departures from recommended FileMan access settings be approved by appropriate personnel.
c) Use of the FileMan utility be monitored periodically for appropriateness.

Concur

As stated in the response to recommendation 1, representatives from the Offices of the Chief Information Officer, the Chief Financial Officer and the Chief Network Officer will meet to determine whether or not a formal VHA directive should be issued to address a wide variety of information security issues. Items included in this recommendation will also be incorporated into that proposed directive. In addition, however, MISS will place added emphasis on the review of FileMan access settings and associated documentation while conducting scheduled facility security site visits. Medical facility staff will also be apprised of OIG's recommended actions during the upcoming training workshops and monthly national conference calls.

Planned September 1996 and Ongoing

9. We recommend that:

a) Management review users with "programmer mode" access privileges for appropriateness and restrict this privilege to only those members of the IRM and ISC staff for which this capability is required for them to perform their job function.
b) Management implement formal monitoring controls over the use of "programmer mode" and monitoring controls to ensure the integrity of IFCAP routines and data is preserved.

Concur with clarification

On some occasions, access privileges are necessary for staff outside of IRM. In those instances, appropriate security clearances for "programmer mode" access privileges are required as stipulated in M-11, Chapter 16. MISS will assure that issues relating to review of programmer access privileges, associated documentation and review of audit trails be communicated to field facility staff via the communication tools described in other sections of this action plan.

Planned September 1996 and Ongoing

October 23, 1996

Assistant Secretary for Management (004)

Draft Report of Audit of the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) System, Phase III
Michael G. Sullivan, Assistant Inspector General for Auditing (52)

We have reviewed your Draft Report of Audit of the Integrated Funds Distribution Control Point Activity, Accounting and Procurement (IFCAP) System, Phase III. Our comments to recommendations one, five, and six, per your request, are provided in the attached document. These comments were shared with officials in Veterans Health Administration and Acquisition and Materiel Management .

We appreciate the opportunity to meet with your staff and ABT Associates, the contract auditors, to clarify the recommendations made. If you have any further questions, please contact Frank W. Sullivan, Deputy Assistant Secretary for Financial Management at (202) 273-5504.

D. Mark Catlett

Attachment

Draft Report of Audit of the Integrated Funds Distribution,
Control Point Activity, Accounting and Procurement (IFCAP) System, Phase III

FINDINGS AND RECOMMENDATIONS

1. Ensure that Appropriate Separation Of Duties is Achieved Over The Initiating, Recording, Reviewing, And Approving Of IFCAP Transactions.

IFCAP controls are designed to separate the functions of initiating, recording, reviewing, and approving of transactions among Control Points, Fiscal Service, and Acquisition & Materiel Management Service (A&MMS) IFCAP users. We observed, however, several instances in which users possessed access to IFCAP which afforded them the ability to perform two or more of these responsibilities. Specifically, we observed the following:

a) An accountant within Fiscal Service possessed access to the Control Point Official, Accounting Technician, and Funds Distribution menus, as well as the security keys normally granted to the Fiscal Chief. Such access may potentially allow the accountant to distribute funds, and create and obligate requests for expenditures for a control point.

b) One Fiscal Chief possessed the ability to assign A&MMS menus and security keys to other IFCAP users. Granting users the capability to assign access to IFCAP menus and security keys for which that user is not responsible may not ensure that appropriate consideration is given to the assignment of those menus.

c) A Management Analyst within Fiscal Service possessed access to both purchase and obligate authority within IFCAP.

Allowing users the capability to perform combinations of initiating, recording, and approving transactions provides the risk that unauthorized transactions may be made and not detected. Unauthorized transactions which are not prevented or detected may result in misappropriation of VAMC funds.

RECOMMENDATION 1:

a) Management periodically review user access within IFCAP to ensure that the duties of initiating, recording, reviewing, and approving transactions may not be performed by the same individuals.

We concur. To assure that an appropriate level of security is maintained, separation of potentially incompatible duties is an important control over data/transaction security and integrity. Allowing free access to the system without effective restrictions runs counter to an efficient security structure. Current established VA policy ensures an appropriate level of security by requiring program management officials to set employee access levels and the Chief, Information

Resources Management Service (IRMS), or their designee to enter user menus and security keys into IFCAP. The requirement for management to periodically review user access should be enforced by VHA through the establishment of appropriate procedures consistent with established policy. This recommendation should be referred to VHA for a plan to resolve this finding.

b) Appropriate monitoring control procedures be established in those instances where conflicts of interest may not be avoided to prevent and/or detect unauthorized transactions from being processed within the system.

We concur. Agencies are required to establish a level of security commensurate with the risk. Having a known security conflict of interest would mandate a periodic independent review or alternate monitoring control procedure.

There are situations when a conflict of interest is unavoidable. The VHA CFO is responsible for granting site exceptions to established security levels where a conflict exists. We will work with the Washington IRM Field Office (IRMFO) to develop a hard copy report to be used by management officials to identify such instances when an exception is granted. A target date for this report has not yet been determined, but it is viewed as a high priority item that will be accomplished as promptly as possible.

5. Implement Monitoring Procedures to Ensure That All Transactions Between IFCAP And FMS Are Processed Completely And Accurately.

The interface between the IFCAP and FMS systems provides for transactions to be processed and updated between the two systems on a daily basis. As with any interface, appropriate procedures need to be developed and placed into operation to ensure that all transactions are processed between the two systems. Examples of conditions that occur that require reconciliations to be performed for the IFCAP and FMS interface include differences in the timing of transactions processed, updated, and reported by each system, and the rejection of transactions processed between the systems.

We noted that reconciliation procedures to ensure all IFCAP interfaced transactions sent to and received by FMS have been processed and updated accurately and timely, vary among VAMCs. Specifically, we had the following observations:

a) The frequency with which reconciliations are performed ranges from twice a month to daily at VAMCs. As a result, transaction balances in IFCAP may not be accurate at given points in time and therefore, not support effective decision-making.

Page 3.

IFCAP Phase III

b) The procedures performed to reconcile IFCAP and FMS balances are felt to be very time consuming and cumbersome by the VAMCs. The time required for performing these reconciliations was reported to have a negative impact on the performance of timely reconciliations.

RECOMMENDATION 5:

We recommend that appropriate monitoring controls be implemented to ensure that all transactions between IFCAP and FMS are completely and accurately processed.

We concur. We will work with VHA to establish appropriate monitoring controls to assure that all transactions between IFCAP and FMS are completely and accurately processed.

6. Strengthen Controls Surrounding The Use Of IFCAP To Ensure That Specific IFCAP Transactions Are Authorized, And Processed Completely And Accurately.

A well controlled internal controls environment is established and maintained through a combination of manual and automated internal control procedures. We noted several opportunities to strengthen the internal controls over the processing of certain IFCAP transactions. Specifically we noted the following:

a) IFCAP provides for inventory adjustments to be processed using the IFCAP "Adjustment Approval Form". These inventory adjustments are actually posted at the time the "Adjustment Approval Form" is created within the IFCAP application. Current procedures require the approval of inventory adjustment transactions by an authorized Approving Official and Accountable Officer. However, the IFCAP application actually posts inventory adjustments upon creation of the "Adjustment Approval Form," without any automated approval required. While a manual review of the inventory adjustment form is still possible, this would occur after the inventory adjustments have been posted. As a result, management's ability to manage inventory balances proactively is diminished.

b) Personnel with responsibility for counting inventory are provided with system generated on-hand inventory totals, prior to conducting each planned physical inventory inspection, through use of the "Warehouse - Inventory Count Form." Providing personnel with IFCAP inventory totals prior to a physical inventory inspection reduces the value of an independent verification of balances through physical inspection, and weakens the control over this process. As a result, management's control procedure to rely on physical inspections to verify the accuracy of inventory totals may not be effective.

Page 4.

IFCAP Phase III

c) IFCAP transactions processed through the General Supply Fund, including purchase orders, may be authorized and obligated by Purchasing Agents without Fiscal Service review. The absence of a control requiring Fiscal Service approval of General Supply Fund transactions, prior to obligation of the funds, restricts the ability of the Fiscal Service to approve and manage all of the financial obligations of the VAMC.

d) The functionality to automate the recording and tracking of goods ordered and received by a VAMC but not obligated within the system exists in IFCAP as an optional feature, which can be used at the discretion of each VAMC. At stations visited, manual procedures were being used for this process. Without controls designed to ensure that all inventory is identified and reported, the ability of management to accurately report total inventory on hand is reduced.

RECOMMENDATION 6:

In order that management may gain additional assurance that all IFCAP transactions are authorized and processed completely and accurately, we recommend the following:

a) A review of the controls over processing of "Inventory Adjustment Forms" should be performed to determine the importance to the VA of approving inventory adjustments prior to being posted in IFCAP. If it is determined that approval of inventory adjustments prior to update in IFCAP is important, we recommend IFCAP be modified to require an automated review of these forms prior to update.

We concur. We have analyzed the situation, the procedure currently in use, and have decided that no change is necessary.

b) Inventory totals in IFCAP should be removed from the "Warehouse Inventory Count Form" used by personnel performing physical inventory inspections.

We concur. Personnel counting inventory should not have on-hand inventory totals. Resolution of this recommendation may require changes to IFCAP. We will address any required system changes and completion dates with the Washington IRM Field Office and ensure that any required changes are accomplished promptly.

c) A review of the controls over the General Supply Fund transaction processing should be performed to determine the importance to the VA of having Fiscal Service review these transactions. If it is determined that Fiscal Service approval of General Supply Fund transactions is desired, we recommend IFCAP be modified to require an automated review of these transactions prior to update.

Page 5.

IFCAP Phase III

We concur. The DAS for Acquisition and Materiel Management is responsible for the Supply Fund and Fiscal Service has no involvement. Again, we will not change current procedures.

d) An emphasis should be placed on the need to use the functionality in IFCAP to record goods received prior to fiscal obligations.

We concur. We will emphasize to VHA the need to utilize the features in IFCAP which allow the automated tracking of goods delivered before an obligation exists.

FINAL DISTRIBUTION

VA DISTRIBUTION

Secretary (00)
Under Secretary for Health (105E)
Assistant Secretary for Management (004)
Assistant Secretary for Congressional Affairs (009)
Deputy Assistant Secretary for Public Affairs (80)
Deputy Assistant Secretary for Acquisition and Materiel Management (90)
Deputy Assistant Secretary for Congressional Affairs (60)
Deputy Assistant Secretary for Financial Management (047)
Deputy Assistant Secretary for Information Resources Management (045)
Deputy Assistant Secretary for Public and Intergovernmental Affairs (002)
Network Directors, VISN 1-22
Director, VAMC Houston (580/00)
Director, VAMC Salt Lake City (660/00)
Director, VAMC Altoona (503/00)
Director, VAMC Minneapolis (618/00)
Director, VAMC Long Beach (600/00)
Director, VAMC Salem (658/00)
Director, VAMC West Palm Beach (548/00)

NON-VA DISTRIBUTION

Office of Management and Budget
U.S. General Accounting Office
Congressional Committees:

- Chairman, Senate Committee on Veterans' Affairs
- Ranking Member, Senate Committee on Veterans' Affairs
- Chairman, House Committee on Veterans' Affairs
- Ranking Democratic Member, House Committee on Veterans' Affairs
- Chairman, Committee on Governmental Affairs
- Ranking Member, Committee on Governmental Affairs
- Chairman, Committee on Government Reform and Oversight
- Ranking Member, Committee on Government Reform and Oversight
- Chairman, Subcommittee on VA, HUD, and Independent Agencies, Senate Committee on Appropriations
- Ranking Member, Subcommittee on VA, HUD, and Independent Agencies, Senate Committee on Appropriations

Chairman, Subcommittee on VA, HUD, and Independent Agencies, House Committee on Appropriations

Ranking Member, Subcommittee on VA, HUD, and Independent Agencies, House Committee on Appropriations