

September 1997

FINANCIAL MANAGEMENT

Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls





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

Accounting and Information
Management Division

B-277418

September 9, 1997

The Honorable William S. Cohen
The Secretary of Defense

Dear Mr. Secretary:

The Department of Defense (DOD) Military Retirement Trust Fund was authorized by Public Law 98-94 for the accumulation of funds to finance, on an actuarially sound basis, DOD's liabilities for military retirement and survivor benefit programs. The DOD Office of Inspector General (DOD IG) audited the Fund's financial statements for fiscal years 1995 and 1996 in accordance with the requirements of the Chief Financial Officers (CFO) Act of 1990, as expanded by the Government Management Reform Act of 1994 (GMRA), and rendered an unqualified opinion on those statements on May 5, 1997. Also, we will audit the consolidated financial statements of the federal government beginning with fiscal year 1997. With total actuarial liabilities of \$548 billion as reported in its financial statements for fiscal year 1996, the Fund is expected to be material to the consolidated governmentwide financial statements.

In preparation for our audit of the consolidated governmentwide financial statements, we contracted with an independent public accounting firm, KPMG Peat Marwick LLP, to review (1) the methods and assumptions used by the DOD Office of the Actuary to calculate the Fund's pension liability as of September 30, 1996, and (2) the effectiveness of general electronic data processing (EDP) controls at the computer processing locations managed by the Defense Manpower Data Center that are responsible for receiving, formatting, and processing the actuarial information. These two areas are critical to verifying the reasonableness of the Fund's reported liabilities.

In order to rely on the work of the KPMG specialists, we

- evaluated the qualifications and independence of the review staff;
- reviewed and approved the contractor's approach plans and work programs;
- attended key meetings between the contractor and DOD personnel; and
- reviewed the contractor's working papers to determine (1) the nature, timing, and extent of work performed, (2) the extent of quality control methods used, and (3) whether evidence in the working papers supported

the contractor's conclusion concerning the reliability of the Fund's actuarial liability and related computer controls.

We performed our oversight of KPMG's work from November 1996 through May 1997, in accordance with generally accepted government auditing standards. DOD provided written comments on a draft of this report. These comments are presented and evaluated in the "Agency Comments and Our Evaluation" section and are reprinted in appendix II.

To avoid duplication of effort, we made KPMG's results available to the DOD IG for its reliance in performing the required fiscal year 1996 financial statement audit and in rendering its opinion on May 5, 1997. Appendix I presents KPMG's report to us on the results of its work.

Results in Brief

Based on our review, we concur with KPMG's conclusion that the methodology and actuarial assumptions used by the DOD Office of the Actuary to calculate the pension liability as of September 30, 1996, and the annual actuarial activity for the Fund were reasonable and reliable.

We also concur with KPMG's identification of numerous control weaknesses related to (1) the data gathering and preparation process and (2) EDP activities. Due to the serious nature of the computer-related weaknesses identified, we agree with KPMG's conclusion that there is a lack of overall security administration and management governing access to Fund data files.

In particular, DOD has not adequately implemented security policies and procedures, controlled the ability of computer programmers to make changes to systems, and controlled access to information on pension fund participants. Such uncontrolled access affects other sensitive personal and career-related information as well.

The computer that houses the Fund's data files also stores information on social security numbers, pay rates, child and spousal abuse allegations, and medical test results for both active duty and retired personnel. Although DOD regulations require that sensitive data be housed only on computers meeting specific security guidelines, the Fund processing sites reviewed by KPMG do not comply with those guidelines. Despite the weaknesses identified, KPMG believed that a material misstatement of the pension liability was unlikely to occur because of compensating controls

that hinge largely on the experience and tenure of staff in the Office of the Actuary.

We agree that compensating controls currently exist in the Office of the Actuary but caution DOD against long-term reliance on controls that depend largely on the retention of a few key employees.

Actuarial Data Gathering and Preparation Process Control Weaknesses

Although the actuarial results were reasonable and reliable for fiscal year 1996, weaknesses exist in the controls over the data gathering and preparation process. Most notably, this process is not adequately documented and, as a result, is heavily dependent on the knowledge of experienced staff members. If significant staff changes were to occur, the annual data update—which is critical to determining the pension liability—might not be performed timely or correctly.

Also, as part of the data preparation process, the Office of the Actuary must estimate the number of eligible inactive reservists because complete data are not provided for inactive reservists who may have earned a vested benefit but have not yet begun to receive benefit payments. Even though the number is small in comparison to total retirees and such an estimate probably would not materially affect the results, DOD should strive for complete and accurate data in order to ensure the correct calculation of its actuarial liabilities. In addition, the program used to calculate the pension liability does not allow the comparison of the actual results using current actuarial estimates and assumptions against the current anticipated results. Such comparison is a standard actuarial process.

Instead, the actuary can only compare, for reasonableness, actual results of the current year calculation in total against prior year valuations. As a result, if prior year calculations were in error, current and future years' calculations could be consistent but also incorrect. Further, no formal documentation exists for this program nor for the data input process and data flow organization/layout of the primary valuation spreadsheet. Here again, the process is dependent on the knowledge of current key staff members.

General EDP Controls Weaknesses

Significant weaknesses related to EDP access controls, security policies and procedures, and program change controls expose the Fund's systems to unnecessary risk and diminish the reliability of its financial management information. Access to pension fund participant information

was not restricted to only those who required such access to perform their jobs. In addition, the activities of individuals who were permitted access to read or modify participant information were not adequately monitored. For example, security violations were not being logged, the ability to use previous passwords was not limited, and over 200 users were permitted to read all data sets on the system. As a result, DOD did not have reasonable assurance that the confidentiality of the data was protected.

Security policies and procedures were either not formalized at data processing sites or, where they were formalized, the sites' daily operations were not in compliance. Many of the control features of the access control software were not activated or the control parameters selected did not adequately restrict access to only authorized users. For example, procedures for both creating and deactivating user accounts were found to be inconsistent and lacking documented guidance.

Features intended to identify users and their related computer activity (audit trails) were not enabled; therefore, if unauthorized activity did occur, there would be no system-generated audit trail to assist in a subsequent investigation. For example, 22 systems users were able to delete and modify files within a component of the operating system that is intended to serve as an audit trail for security-related events. As a result, they could inactivate the parameter that enables the auditing of security events. Typically, system users would not be able to change or delete the audit trail function.

There were no formal controls governing how changes to systems could be made or who could make them. For the application system that calculates the pension liability, no comprehensive change management process has been developed. For the operating systems, although a change management process exists, it lacks procedures to ensure that changes are documented, tested, reviewed, and approved. Consequently, changes could be introduced to the operating system that would facilitate unauthorized access and those changes may not be detected promptly.

DOD has not developed, tested, and implemented a comprehensive disaster recovery plan at the sites that process Fund data. Should a disaster occur, DOD has no assurance that the computer facilities and operations or the actuarial operations necessary to support the Fund could be restored in a timely manner. The Fund may be at further risk since the application that performs the actuarial calculations—an application that may be sensitive

to date changes—has not yet been assessed for Year 2000 impact.¹ In assessing risk, DOD must determine the impact of the year 2000 on its systems and applications and initiate realistic contingency plans to ensure continuity of business processes if systems or applications fail to operate at the turn of the century.

Recommendations

We concur with all of the recommendations made by KPMG to address the actuarial process and EDP general controls weaknesses identified during the review. To improve the actuarial process, we recommend that you ensure that the Office of the Actuary

- documents annual data preparation and processing steps in a formal, detailed manual;
- determines the availability of complete data on inactive reservists;
- tests a sample of current valuation results independently from prior year results; and
- evaluates the efficiency of using the current spreadsheet analyses and documents those analyses.

To address the EDP general controls weaknesses, we recommend that you ensure that the Defense Manpower Data Center

- modifies the security program's parameters to ensure participants' data and actuarial programs are protected and that security requirements comply with regulations;
- implements security features and parameters to ensure that unauthorized access to systems is reduced and that audit trails are activated and protected from unauthorized editing;
- develops (or modifies) and implements security policies and procedures to ensure that (1) all users are authorized and have only the necessary access to facilities and data, (2) such access is reviewed periodically and removed promptly when warranted, and (3) access violations are researched;
- develops and implements comprehensive change management procedures governing changes to both the Fund's application programs and related operating systems;
- designs, develops, tests, and implements a comprehensive disaster recovery plan; and

¹The Year 2000 problem is rooted in the way dates are recorded and computed in many computer systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997. With this two-digit format, the year 2000 is indistinguishable from 1900, 2001 from 1901, and so forth. As a result, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999.

-
- formally assesses and documents the risk of the Year 2000 impact on the actuarial application and prepares contingency plans, if needed, to ensure operations are not disrupted.

In addition, KPMG made other suggestions to address less significant weaknesses and provided them to DOD personnel under separate cover. We concur with those suggestions as well.

Agency Comments and Our Evaluation


In written comments on a draft of this report, DOD concurred with our recommendations to improve its actuarial process and EDP general controls. DOD's response (see appendix II) cited numerous planned corrective actions to address the individual components of those recommendations. DOD's corrective action plan addresses the weaknesses cited in our report.

You are required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Reform and Oversight within 60 days of the date of this report. You must also send a written statement to the House and Senate Committees on Appropriations with the agency's first request for appropriations made over 60 days after the date of this report.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Armed Services, the House Committee on National Security, the Senate Committee on Governmental Affairs, and the House Committee on Government Reform and Oversight and the Director of the Office of Management and Budget. We are also sending copies to the Acting Under Secretary of Defense (Comptroller)

and the DOD Inspector General. Copies will be made available to others upon request. Please contact Molly Boyle, Assistant Director, Defense Audits, on (202) 512-9524 if you or your staff have any questions.

Sincerely yours,

A handwritten signature in black ink, reading "Gene L. Dodaro". The signature is written in a cursive style with a large, stylized initial "G".

Gene L. Dodaro
Assistant Comptroller General

Review of the Military Retirement Trust Fund's Actuarial Model

KPMG Peat Marwick LLP

2001 M Street, N.W.
Washington, D.C. 20036

Telephone 202 467 3000

Telefax 202 833 1350

May 15, 1997

Mr. Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division
U.S. General Accounting Office

Dear Mr. Dodaro:

This report presents the results of our review of the Military Retirement Trust Fund's (MRTF) actuarial model under contract No. 6130007, Task Order 96-12. Our work included reviewing the actuarial assumptions, methods, systems, and related controls used by the Department of Defense (DoD) Office of the Actuary to calculate MRTF's pension cost liabilities and annual actuarial activity for financial statement and other reporting purposes. Our work also included a review of the general control environment at the electronic data processing (EDP) locations that are responsible for receiving, formatting, and processing the actuarial information.

MRTF's estimated actuarial liability was calculated as approximately \$548 billion for fiscal year 1996 and, therefore, is expected to be material to the consolidated government-wide financial statements, which the General Accounting Office (GAO) is required to audit for fiscal year 1997. In anticipation of this audit effort, GAO requested that we provide them with an independent assessment of MRTF's fiscal year 1996 actuarial liability calculations, including relevant assumptions and related computer system controls, in time to effect improvements or changes if necessary. To avoid duplication of work, GAO made KPMG's results available to the DoD Office of the Inspector General (IG) for its reliance in performing the required fiscal year 1996 audit of MRTF's financial statements.

Results in Brief

Based on the procedures performed and the results obtained, we believe that the methodology and actuarial assumptions used by the DoD Office of the Actuary to calculate the fiscal year 1996 pension liability and annual actuarial activity for MRTF are reasonable and reliable. The economic and demographic assumptions include such items as interest rates, cost of living adjustments, salary increases, retirement ages, and mortality rates. The assumptions used compared favorably to those used by the Civil Service Retirement Fund and the Social Security Administration. Additionally, the assumptions are consistent with guidelines specified in Federal

Member Firm of
Klynveld Peat Marwick Goerdeler

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

Financial Accounting Standard No. 5 and the Financial Accounting Standards Board Statement No. 35. The methodology used to apply the assumptions to the participant data determines the final liability. Specific steps involve data preparation and evaluation, modifications to reflect annual programming changes and occasional changes in assumptions and benefit levels, and analysis of results for accuracy.

Although we found the results to be reliable, the current data preparation process relies heavily on experienced staff members and has not been adequately documented. As a result, if significant staff changes were to occur, the required annual data update might not be performed timely or correctly, and the integrity of the updated data is significant to the valuation of pension liabilities.

We also found other, less significant problems related to the accuracy of information concerning certain reservists and the availability of spreadsheet analysis documentation.

In our review of the EDP general controls over the systems which process MRTF data, we identified three significant areas of weakness that expose the systems to unnecessary risk and diminish the reliability of MRTF's financial management information. The effect of these weaknesses, when considered in the aggregate, has led us to conclude that the access controls at MRTF data processing sites are not in compliance with federal security standards for sensitive information.

First, access to information concerning pension fund participants was not restricted to only those who required such access to perform their job functions. In addition, the activities of individuals who were permitted access to read or modify participant information were not adequately monitored. Consequently, DoD management did not have reasonable assurance that the confidentiality of the data was protected.

Second, security policies and procedures were either not formalized at data processing sites or, where security policies and procedures were formalized, the sites' daily operations were not in compliance. Many of the control features of the access control software were not enabled or the control parameters selected did not adequately restrict access to only authorized users. Features intended to identify users and their related computer activity (audit trails) were not enabled; therefore, if unauthorized activity did occur, there would be no system-generated audit trail to assist in a subsequent investigation.

Third, there were no formal controls governing how changes to operating systems could be made or who could make them. Consequently, changes could be introduced to the operating system that would facilitate unauthorized access and those changes may not be detected in a timely fashion. We also identified other, less significant weaknesses dealing with computer program modifications and disaster recovery plans.

Because the computer related weaknesses we identified were so pervasive and fundamental, we concluded that there is a lack of overall security administration and management governing access

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

to MRTF data files. However, we believe that it is unlikely that material misstatements of the pension liability would occur because of the following compensating controls:

- the experience and long tenure of the Office of the Actuary employees,
- the manual processes relating to the production and review of actuarial data, and
- the nature of the calculation itself (i.e., an estimate of the future liability value of the pension fund as opposed to specific payment amounts to beneficiaries.)

Background

DoD's Office of the Actuary in Rosslyn, Virginia, performs an annual valuation of pension liabilities for use in MRTF financial statements and other reports to the Congress. DoD personnel and payroll offices supply the required data for pension plan participants to the Defense Manpower Data Center (DMDC) in Monterey, California (West). DMDC West passes the data through various edit routines to ensure completeness, accuracy, and reasonableness; initiates corrective action to resolve data errors; and stores the output data on magnetic media at the Naval Postgraduate School (NPS), which is also located in Monterey.

NPS is an academic institution whose emphasis is on study and research programs relevant to Navy interests and other DoD areas. Many computer-based and professional support services are provided by the NPS Computer Center to a variety of DoD and other users. The Computer Center houses two mainframe computers, one of which is an AMDAHL 5995-700A which utilizes IBM's operating system and access security software. Connectivity is provided via mainframe terminals, PC compatible machines, or dial-up capability. This machine is used for interactive computing, batch production, and transaction processing. Data supporting the pension liability calculation program, known as GORGO, are processed and stored on this machine.

The GORGO application is a FORTRAN-based program used by the DMDC in Arlington, Virginia (East) to sort, group, and tabulate the edited participant data provided by DMDC West into the format required by the Office of the Actuary. The Office of the Actuary downloads GORGO processed data into a variety of actuarial models and, using various sets of assumptions, produces the pension liability amount for MRTF.

In addition to MRTF data, DMDC West archives other databases and files for DoD on the AMDAHL mainframe. The information stored on this computer can be divided into the following five categories: personnel, pay, financial, training, and other. Many of these files contain sensitive personal or career-related information for both active duty and retired personnel, including social security numbers, pay rates, child and spousal abuse allegations, and medical test results. DoD regulations require that sensitive data be housed only on computers meeting specific security guidelines. Specifically, compliance with the "C2" level of security as defined by DoD 5200.28-STD, "Trusted Computer System Criteria," provides for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of users and the

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

actions they initiate. Users are to be individually accountable for their actions through log-in procedures, auditing of security relevant events, and resource isolation. In addition, Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," establishes a minimum set of controls to be included in federal automated information security programs.

Objective, Scope, and Methodology

Under Task Order 96-12, the objective of our work was to assist GAO with an independent assessment in two specific areas. The first was to provide actuarial expertise to assist GAO in determining whether the methodology, calculations, and assumptions used by the DoD Office of the Actuary to estimate the fiscal year 1996 pension liabilities for the MRTF are reasonable and reliable. The second was to provide information technology expertise in assisting GAO in determining the effectiveness of the EDP general control environment at the computer processing locations that are responsible for receiving, formatting, and processing the actuarial information.

We performed field work for a period covering 7 weeks (November 19, 1996, through January 3, 1997) at all necessary locations. The actuarial portion of our work covered the following four basic areas:

- participant data gathering and preparation process,
- actuarial methods and assumptions,
- actuarial applications, including GORGO and related spreadsheets, and
- communication of results.

The EDP general controls review covered five basic components:

- security,
- system design, development, and modification, including program change controls,
- segregation of duties,
- system software, and
- service interruption.

We utilized all appropriate and necessary techniques to complete our review. These included inquiry and observation, review and testing of applicable actuarial and EDP control documentation, comparison to benchmarks and standards, judgmental samples, recalculation of results, and, where required, utilization of computer software to evaluate the settings of certain operating system parameters. We were given access to all files, computers, facilities, and personnel necessary to observe and verify information.

Our preliminary findings were presented to and discussed with DoD personnel at applicable locations. Without exception, management at each location verbally concurred with the findings. Management was not requested to provide a written response.

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

Finally, an oral briefing summarizing our notices of findings and recommendations was presented to representatives of GAO, the DoD Office of the Actuary, DMDC East, and the DoD IG.

Summary of Findings

We performed two interrelated reviews--one focused on the actuarial model and related assumptions and the other on EDP general controls. The results of each are summarized in this section, and our recommendations are provided in the last section.

Actuarial Review

Within the actuarial portion of our review, we identified weaknesses in two main areas.

Data gathering and preparation process - The data received by the DoD Office of the Actuary requires extensive preparation prior to use for valuation purposes. The correct completion of this preparatory process is vital to the proper calculation of liabilities. The current staff is experienced and completes the tasks based on established criteria. However, we found that the current day-to-day procedures are not well documented. This lack of documentation increases both the reliance on certain key individuals and the risk of errors in actuarial calculations going undetected should staffing changes occur. The proper level of documentation will allow timely continuation of work even in the event of staffing changes.

Complete and accurate valuation data is required to ensure the correct calculation of liabilities. However, we found that data are not available for inactive reservists who may have earned a vested benefit but have not yet begun to receive benefit payments. As a result, the Office of the Actuary must estimate the number of eligible inactive reservists. Because the number of vested, inactive reservists are small in relation to the total MRTF population, such an estimate, while not 100 percent accurate, will not materially affect results.

Actuarial applications - In verifying liabilities, the results of actuarial estimates and assumptions are checked against prior valuations for reasonableness. They are not tested against current anticipated results. Generally, valuation software provides a feature which details current year calculations. This enables the actuary to verify that calculations are in accordance with given assumptions and methods. The GORGO program was thoroughly tested when introduced but does not produce current year sample results. The risk is that if the prior year's calculation is incorrect, current and future years' calculations may be consistent but also incorrect.

The actuarial systems include GORGO and spreadsheet analysis. Because there are many recurring annual processes and occasional one-time changes, documentation is essential. We found that the GORGO system has no formal documentation, and written procedures

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

do not exist that describe the data input process or data flow organization/layout of the primary valuation spreadsheet. Consequently, as indicated earlier, the Office of the Actuary relies heavily on the knowledge of several key, long-tenured employees. Additionally, the current spreadsheet analysis is maintained in a large file with comments in various sections. Current software features may be used to create a more efficient spreadsheet with comments easier to find. In general, the lack of system documentation and operational procedures may cause both inefficiencies in making changes to the GORGO application and errors in the spreadsheet valuations, should personnel changes occur.

EDP General Control Review

As noted earlier, the EDP general control review disclosed a number of control weaknesses. We discussed 27 findings in this area with DoD personnel. The most significant of these are presented below.

Implementation of access control software - Resource Access Control Software (RACF) is the access control software implemented on the AMDAHL computer system supported by NPS. The purpose of RACF is to control access to computer resources and data sets. RACF is capable of providing access controls that meet or exceed the requirements of the "C2" level of security as defined by DoD 5200.28-STD, "Trusted Computer System Criteria."

The review of controls over the administration of logical security of the operating system (i.e., the security that facilitates access to the system) at NPS identified weaknesses which included but were not limited to the following:

Certain key RACF security features had not been activated. For example, features that would permit the following key security measures were not enabled: logging of security violations, automatically protecting all data sets, and limiting the use of special programs that can directly modify the operating system and/or application data. Also, because RACF profiles have not been defined for all data sets, system libraries without a RACF profile can be accessed by any of the over 200 users defined to RACF.

RACF user controls have not been effectively implemented. Specifically, (1) RACF user accounts that are not used for an extended period of time are not automatically disabled, (2) the RACF option to limit the ability of users to use a previous password has not been enabled, (3) the RACF option to automatically disable a user account after a set number of unsuccessful log-on attempts has not been enabled, and (4) the RACF option to require and enforce minimum password length and syntax has not been defined.

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

The RACF special attribute that allows users to define security rules is assigned to an excessive number of user accounts. Seven user accounts have been assigned this special attribute, which generally is limited to a primary security administrator and usually no more than two backup security administrators.

The RACF read access rule has been set to permit over 200 users to read all data sets on the system. In addition, the access rules for three libraries were set to "alter," allowing all users to add, modify, or delete the programs or libraries.

The RACF default passwords, which are vendor supplied and widely known, for switching the RACF data sets and disabling the RACF security system have not been changed.

Systems audit trail - The System Management Facility (SMF) is a component of the operating system that documents information about specific events. These events may be related to security events, access to data sets, access by users to the operating system, and processing system tasks. SMF plays an integral role in access control and security administration by serving as the audit trail for significant actions associated with system activity. Our review identified the following control issues related to the systems audit trail: (1) all users defined to the SMF files are permitted to read the SMF files, and 22 users defined as computer center systems and operations staff can delete and modify SMF files, (2) the RACF parameter to allow the auditing of security events is not enabled, and (3) certain SMF record types that would document key events are not collected.

Controls over related computer system - The VM/XA computer system is used by the NPS to provide access to the AMDAHL computer system. DMDC West staff and NPS faculty, staff, and students are granted accounts on the VM/XA computer system. These users are permitted to request the running of programs on the operating system that runs the GORGO application. Although the operating system uses RACF to determine if the user submitting the job is authorized to do so, we found that numerous operating system security features had not been enabled. The capabilities that are missing include, but are not limited to, (1) user account administration, (2) user password administration, including encryption of passwords, automatic suspension of accounts, and monitoring of user activities, and (3) recording/monitoring and reporting of significant security events.

Security policies and procedures - We found several areas where overall security policies and procedures should be improved and formalized. For example, at both DMDC and NPS, user account administration procedures should be improved. With respect to user account creation, procedures for identification, validation of new user access requests--including dial-up access, and communication of requests to user registration are not consistent. Conversely, when computer center users leave, transfer, or are terminated, there is no standard documented procedure to inform user registration and ensure that the related accounts are deactivated and/or deleted. There is also no formal periodic

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

monitoring of user accounts to verify that the actual level of access is consistent with the approved level of access.

Other weaknesses in security policies and procedures include (1) a security risk analysis has not been performed on a periodic basis, (2) a formal security awareness program does not exist, and (3) physical access controls governing access to GORGO related data centers and back-up tapes are not sufficient to prevent unauthorized access.

Change management process - A comprehensive change management process governing modifications to the GORGO application has not been developed and implemented. In addition, changes to the GORGO application are made in the production environment rather than in a separate and controlled test environment.

Although NPS does have a process for managing changes to the operating systems, we found that the change management process, including installation and maintenance, lacks procedures to ensure that such changes are documented, tested, reviewed and approved. The change control process should ensure that changes to the operating systems do not introduce weaknesses that provide ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the operating systems and gain access to unauthorized resources.

Other weaknesses - A comprehensive disaster recovery plan, including processing priorities, has not been developed, tested, and implemented at either of the DMDC sites or NPS and an analysis of the year 2000¹ impact on MRTF data has not been documented nor have detailed action plans been developed.

The effects of these findings both individually and in the aggregate are twofold. First, DoD has no assurance that (1) GORGO data and programs are restricted only to those who require such access to perform their job function, (2) operating system security controls are adequate to prevent or detect attempts to gain access to the operating system and the GORGO application by unauthorized individuals, and (3) unauthorized access to or dissemination of GORGO related data will not occur, or if such actions should occur, that they would be detected in a timely manner. Second, the physical and logical controls in place are not in compliance with OMB Circular A-130 and do not provide for the minimum capabilities required of a computer system to meet the "C2" level of security as defined by DoD.

¹The year 2000 problem is rooted in the way dates are recorded and computed in many computer systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997. With this two-digit format, the year 2000 is indistinguishable from 1900, 2001 from 1901, and so on. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999.

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

 Peat Marwick LLP

In addition, should a disaster occur to either of the DMDC sites or to the NPS data center, DoD has no assurance that computer facilities and operations or the actuarial operations could be restored in a timely manner. DoD also has not assessed the year 2000 impact on the GORGO application nor developed a project plan to mitigate related problems.

Conclusions and Recommendations

Although we found that the methodology and assumptions used by the DoD Office of the Actuary to calculate the fiscal 1996 pension liabilities and annual actuarial activity for the MRTF are reasonable and reliable, the number, significance, and fundamental nature of our EDP findings lead us to conclude that there is a lack of overall security administration and management governing access to information stored on the computer that processes MRTF data. Consequently, unauthorized users may alter, modify, or delete programs and related data files and confidential data may be compromised or corrupted. Therefore, we recommend that DoD take the following actions to improve its general controls:

Actuarial Review

Document annual data preparation and processing steps in a formal, detailed manual. This manual should detail data sources, full data capabilities of DMDC West, expected condition of data received from DMDC West, and all usual procedures involved in data preparation.

Determine the availability of complete data on inactive reservists. Interim processes should include the continued monitoring of estimates against actual experience. Test a sample of current valuation results independently from prior year results, in conjunction with current procedures.

Evaluate the current spreadsheet analysis to determine if software features are being used efficiently. In addition, document the GORGO and spreadsheet analyses, including details on the steps necessary to produce final MRTF liabilities.

EDP General Control Review

Modify RACF security parameters to ensure that GORGO data and programs are protected and that security requirements are compliant with both OMB Circular A-130 and DoD Standard 5200.28.

Implement additional security features and parameters provided by the operating systems to ensure that unauthorized access to system resources and data on the NPS systems is reduced and that audit trails are activated and protected from unauthorized editing.

Appendix I
Review of the Military Retirement Trust
Fund's Actuarial Model

KPMG Peat Marwick LLP

Develop, modify, and implement security policies and procedures to ensure that (1) all users are authorized and have access only to the facilities and data required to perform their job function, (2) such access is reviewed periodically for appropriateness, and, when warranted, access is removed timely, and (3) access violations are researched.

Develop and implement comprehensive change management procedures governing changes to both the GORGO application and related operating systems. Procedures should ensure that changes are authorized; made, tested, and reviewed in a secure test environment; approved by the user prior to implementation in the production environment; and adequately documented.

Design, develop, test, and implement a comprehensive disaster recovery plan. The plan should encompass all processing platforms and identify any processing priorities and related time parameters. In addition, the plan should include all necessary administrative and operational (e.g., non-computerized) procedures that are necessary to compute the MRTF liability.

Modify data center physical access and tape back-up procedures to ensure that facilities are adequately protected against unauthorized individuals and that back-up files are stored off-site in a secure location.

Formally assess and document the year 2000 impact on the GORGO application. Once the assessment is complete, a project plan should be developed that outlines the resources required, cost, time lines, and review dates.

We also made other suggestions to address the less significant weaknesses we found. We provided documentation on all of these weaknesses and suggested improvements to DoD personnel under separate cover.

KPMG Peat Marwick LLP

Comments From the Department of Defense



PERSONNEL AND
READINESS

OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D. C. 20301-4000



JUL 24 1997

Gene L. Dodaro
Assistant Comptroller General
Accounting and Information
Management Division
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report "FINANCIAL MANAGEMENT: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls," dated July 11, 1997 (GAO Code 918889/OSD Case 1411).

In this report, GAO made one recommendation with respect to improving the actuarial process and one recommendation concerning the electronic data processing general controls. The DoD concurs with both of these recommendations. The first recommendation had four components; the second had six. Detailed comments on each component of the recommendations are enclosed.

The Department appreciates the opportunity to comment on the draft report.

Sincerely,

Jeanne B. Fites
Deputy Under Secretary of Defense
Program Integration

Enclosure:
As stated



GAO DRAFT REPORT - DATED JULY 11, 1997
OSD Case 1411, GAO Code 918889

“FINANCIAL MANAGEMENT: REVIEW OF THE MILITARY RETIREMENT TRUST
FUND’S ACTUARIAL MODEL AND RELATED COMPUTER CONTROLS”

DEPARTMENT OF DEFENSE COMMENTS ON THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense, to improve the actuarial process, ensure that the Office of the Actuary (1) documents annual data preparation and processing steps in a formal, detailed manual; (2) determines the availability of complete data on inactive reservists; (3) tests a sample of current valuation results independently from prior year results; and (4) evaluates the efficiency of using the current spreadsheet analyses and documents those analyses. (p. 5/GAO Draft Report)

DoD RESPONSE: Concur. Detailed comments on each component follow:

- (1) The Office of the Actuary recognizes that there is no single document outlining the data preparation and processing steps for performing the annual valuation of the Military Retirement System (MRS), although separate documentation for the various stages does exist. This documentation has been improved in recent months. In addition, the Office of the Actuary has recently let a contract for a private actuarial consulting firm to develop new valuation software. The contract stipulates a formal, detailed manual as a deliverable, which should resolve the documentation problem. Due to delays with the contracting process, this project is now expected to be completed for the valuation as of September 30, 1998. While it would be desirable for the documentation to be sufficient for an entire new staff of actuaries to take over in the absence of the current staff, there are too many steps involved for such a capability to be achieved.
- (2) Reserve data required for the valuation of the MRS, which is kept at DMDC-West, was virtually non-existent ten years ago. The Services all undertook a sustained effort to improve the quality of the data. For a number of years, the Office of the Actuary prepared semi-annual reports tracking the quality of the necessary data elements. The data now appear to be accurate and complete enough to be tested in the valuation. However, the current valuation program, which was written when the reserve data was still extremely unreliable, does not incorporate the improved data directly in the valuation. The new valuation software referred to above will be written to use reserve data directly, although there will be a transition period to reconcile the results of the two valuation programs. In addition, there are complications related to factors other than the

quality of the data. The project is currently scheduled to be completed for the valuation as of September 30, 1998.

- (3) When the current valuation program was written, it was extensively tested and audited by an independent actuarial consulting firm, including testing samples of valuation results outside the program. Since that time, the Office of the Actuary has relied on year-to-year reasonableness checks in its validation process. The DoD has stipulated that the new valuation software under contract include the ability to sample current valuation results independently from prior year results. The project is currently scheduled to be completed for the valuation as of September 30, 1998.
- (4) The Office of the Actuary continually seeks to improve the valuation process. With respect to the spreadsheet analyses, this has included such improvements as including macros to automatically perform functions which were previously done manually, distinguishing input items to the spreadsheets from calculated items, and moving separate pages of the valuation spreadsheet to individual worksheets. Many of the improvements have been accomplished since conferences with the auditors last winter. In keeping with the current actuarial and computing environments, the consulting firm hired to develop the new valuation software will explore making the entire valuation spreadsheet-based, rather than relying on mainframe software. The consulting firm will develop the software to be as efficient as possible. This project is expected to be completed for the valuation as of September 30, 1998.

RECOMMENDATION 2:

The GAO recommended that the Secretary of Defense, to address the electronic data processing (EDP) general controls weaknesses, ensure that the Defense Manpower Data Center (DMDC) (1) modifies the security program's parameters to ensure participants' data and actuarial programs are protected and that security requirements comply with regulations; (2) implements security features and parameters to ensure that unauthorized access to systems is reduced and that audit trails are activated and protected from unauthorized editing; (3) develops (or modifies) and implements security policies and procedures to ensure that all users are authorized and have only the necessary access to facilities and data, such access is reviewed periodically and removed promptly when warranted, and access violations are researched; (4) develops and implements comprehensive change management procedures governing changes to both the Fund's application programs and related operating systems; (5) designs, develops, tests, and implements a comprehensive disaster recovery plan; and (6) formally assesses and documents the risk of the year 2000 impact on the actuarial application and prepares contingency plans, if needed, to ensure operations are not disrupted. (p. 5/GAO Draft Report)

DoD RESPONSE: Concur. Detailed comments on each component follow:

- (1) The DMDC has been working on a comprehensive security plan for the past six months with a private sector contractor who has been reviewing DMDC's current security practices and has made recommendations that address DMDC's security vulnerabilities. The second part of the contract is to assist in implementing EDP controls that will protect all of DMDC's data assets including the actuarial programs. The proposed solutions will be in compliance with the current regulations and are projected for full implementation during the second quarter of FY98.
- (2) The DMDC is addressing the issue of access in multiple ways. For external access control DMDC is purchasing two new terminal servers which require passwords to gain access to the system and which provide access accountability. These passwords are in addition to the passwords required for each on-line account. DMDC will also establish a policy that dictates changing internal account passwords on a more frequent basis. For internal access control the DMDC is finalizing its implementation of the Resource Access Control Facility (RACF) which delineates which individuals are allowed access to DMDC data files and application libraries. The RACF also has an audit trail associated with it. The organizational implementation of RACF is planned for the third quarter of FY98.
- (3) The DMDC has been working closely with its contractor on security procedures. The contract requires that the contractor provide documentation for recommended security procedures which the DMDC will implement.

At the DoD Center, on its interior spaces the DMDC will install, in August 1997, an Automated Facial Recognition System (AFRACS) on the access doors where the DMDC data inventory is stored to severely restrict access. All Network Operations Center spaces have been rekeyed to a unique key held only by systems staff. The DMDC has already installed a new electronic access system which requires a unique card to gain entry to the building. All accesses are recorded in electronic format for review by the security staff. The security system is being further enhanced with a video monitoring and recording system on the interior and exterior of the building.

At the Naval Postgraduate School (NPS) an electronic key lock system controlled by magnetic card proximity readers has been installed on all access points into the data center.

The RACF has the capability of segregating data into "need to access" categories. The DMDC has developed a plan for restricting access to these categories on a requirements basis and will implement their plan coincidental to the

Appendix II
Comments From the Department of Defense

implementation of RACF in the third quarter of FY98. RACF does provide the necessary audit trails for review of accesses made to DMDC data files and libraries.

The DMDC will immediately initiate a plan to periodically review its security procedures.

- (4) The Office of the Actuary has restricted access to the mainframe account housing the valuation program to two staff members. No others are allowed to make changes to the valuation programs on that account. All changes to the current valuation program are made in a separate file by one of these individuals, checked by someone else, and then moved into the valuation program. All changes made to valuation programs are documented. Also, all valuation-related spreadsheets can only be accessed in read-only mode, except by two staff members. These individuals are the only personnel authorized to make changes to the valuation spreadsheets.
- (5) The DMDC has provided three geographically disparate sites for storing its data inventory: the NPS data center for active use, the DoD Center for first stage backup, and the Hill AFB, Ogden, Utah data center for archival backup. The DMDC currently has a computer center under contract to provide computer support for one of its production applications. The contract can be expanded to include disaster recovery services. The DMDC will develop and implement a comprehensive plan that will bring these resources together to accomplish a disaster recovery scenario by September 1998.
- (6) In September 1997, the DMDC will have converted its operation to a new suite of hardware at the NPS data center, including an IBM CMOS processor and a new operating system, OS/390. Both the hardware and the software are Year 2000 compliant. Additionally, the DMDC is addressing the conversion of its tape inventory on the new system to establish compatibility with Year 2000 requirements. The anticipated completion date for the tape conversion project is September 1998.

Ordering Information

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

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

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

<http://www.gao.gov>

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

**Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested
