

Audit



Report

OFFICE OF THE INSPECTOR GENERAL

**CONTROLS OVER ACCESS TO
PERSONNEL AND PAYROLL DATA FOR THE
DEFENSE COMMISSARY AGENCY**

Report No. 94-081

April 11, 1994

Department of Defense

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 614-6303 (DSN 224-6303) or FAX (703) 614-8542.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch, Audit Planning and Technical Support Directorate, at (703) 614-1868 (DSN 224-1868) or FAX (703) 614-8542. Ideas and requests can also be mailed to:

Inspector General, Department of Defense
OAIG-AUD (ATTN: APTS Audit Suggestions)
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

DoD Hotline

To report fraud, waste, or abuse, call the DoD Hotline at (800) 424-9098 (DSN 223-5080) or write to the DoD Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of writers and callers is fully protected.

Acronyms

APCAPS	Automated Payroll, Cost and Personnel System
DBMS	Defense Business Management System
DeCA	Defense Commissary Agency
DFAS	Defense Finance and Accounting Service
DITSO	Defense Information Technology Services Organization
TALE	Time, Attendance, Leave and Earnings



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884**

April 11, 1994

**MEMORANDUM FOR DIRECTOR, DEFENSE COMMISSARY AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE**

**SUBJECT: Audit Report on Controls Over Access to Personnel and Payroll Data for the
Defense Commissary Agency (Report No. 94-081)**

We are providing this report for your information and use. The report discusses the adequacy of controls for accessing personnel and payroll information.

The Director, Defense Commissary Agency, and the Director, Defense Finance and Accounting Service, provided timely comments and adequately addressed all corrective actions recommended in the report. Therefore, no further action is required.

The courtesies extended to the audit staff are appreciated. If you have any questions on this audit, please contact Mr. Robert J. Ryan at (703) 692-3457 (DSN 222-3457) or Mr. John Yonaitis at (703) 692-3446 (DSN 222-3446). Appendix C lists the distribution of this report. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

**Robert J. Lieberman
Assistant Inspector General
for Auditing**

Office of the Inspector General, DoD

Report No. 94-081
Project No. 3LA-2002.03

April 11, 1994

CONTROLS OVER ACCESS TO PERSONNEL AND PAYROLL DATA FOR THE DEFENSE COMMISSARY AGENCY

EXECUTIVE SUMMARY

Introduction. The Defense Finance and Accounting Service provides personnel and payroll services for the Defense Commissary Agency (DeCA) employees in the continental United States and, as of October 1, 1993, maintains the east and west data bases in the Defense Business Management System (DBMS), formerly the Automated Payroll, Cost and Personnel System. Prior to October 1, 1993, the Defense Information Technology Services Organization maintained the DBMS data bases. DeCA stores, regions, service centers, and headquarters personnel enter personnel and payroll data into the DBMS. The future use of DBMS for this function is currently under review.

The internal control weaknesses identified in this report concerning access to the personnel and payroll system currently used by DeCA would be applicable to any subsequent personnel and payroll system used by DeCA.

Objective. The overall audit objective was to determine whether the FY 1993 financial statements for the Commissary Operations Fund are presented fairly and in accordance with generally accepted accounting principles. This report discusses the adequacy of internal controls and DBMS operations for accessing personnel and payroll information.

Audit Results. Access to personnel and payroll subsystems in the DBMS data bases was not adequately controlled. Permitting unrestricted access to both subsystems could result in the unauthorized alteration of records, improper payments, payments to fictitious personnel, and access to Privacy Act information.

Internal Controls. The audit identified material internal control weaknesses. Controls over access to personnel and payroll data and Privacy Act data were inadequate. See Part I for details on internal controls assessed and Part II for a discussion of the weaknesses.

Potential Benefits of Audit. No monetary benefits were identifiable. Other benefits are summarized in Appendix A.

Summary of Recommendations. We recommended that DeCA and the Defense Finance and Accounting Service establish internal controls to restrict the number of employees with access to both the personnel and payroll subsystems, match user identification numbers to active DeCA employees, restrict employee access to the personnel and payroll data, and establish software requiring employees to periodically change their passwords.

Management Comments. DeCA and the Defense Finance and Accounting Service have implemented a process to restrict access to a single subsystem of DBMS, agreed to periodically screen the DBMS to ensure only authorized users have access, created a

separation of duties between personnel and payroll functions, agreed to limit data base access by authorized personnel, and initiated a process to force users to change their initial passwords when they initially log on to the DBMS. Additionally, they are establishing an automated system requiring complete password changes every 90 days. The complete texts of the managements' comments are in Part IV.

Audit Response. We consider the DeCA comments and the Defense Finance and Accounting Service comments to be responsive to the recommendations. Therefore, no further comments are required.

Table of Contents

Executive Summary	i
Part I - Introduction	1
Background	2
Objective	2
Scope and Methodology	3
Internal Controls	3
Prior Audits and Other Reviews	4
Part II - Finding and Recommendations	5
Access to Personnel and Payroll Data	6
Part III - Additional Information	13
Appendix A. Summary of Potential Benefits Resulting from Audit	14
Appendix B. Organizations Visited or Contacted	15
Appendix C. Report Distribution	16
Part IV - Management Comments	19
Defense Commissary Agency	20
Defense Finance and Accounting Service	24

This report was prepared by the Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, Department of Defense.

Part I - Introduction

Background

The Defense Commissary Agency (DeCA) was established on October 1, 1991, as a result of the consolidation of the Military Department commissary systems. DeCA employs about 19,000 civilian personnel within the continental United States, for which the Defense Finance and Accounting Service (DFAS) is responsible for paying wages of about \$380 million from the appropriated Commissary Operations Fund, a part of the Defense Business Operations Fund.

The Defense Business Management System (DBMS), (formerly the Automated Payroll, Cost and Personnel System [APCAPS]), is used to process DeCA's personnel and payroll services for continental United States employees. DeCA enters personnel and payroll data into the east and west data bases of DBMS and determines which employees should receive user access. The DFAS-Columbus Center, Columbus, Ohio, using the DBMS, processes the payment of continental United States employees and performs related accounting functions. Additionally, prior to October 1, 1993, the Defense Information Technology Services Organization (DITSO), Dayton, Ohio, a part of the Defense Information Systems Agency, maintained the east and west data bases of DBMS, including the hardware and the software used to run the systems, controlled user access into the DBMS, and was responsible for the security of the DBMS.

Effective October 1, 1993, Defense Management Report Decision 9-18 transferred the information processing activities from DITSO to the Defense Information Services Organization, a part of Defense Information Systems Agency, and returned the central design activities to the original owners. With Defense Management Report Decision 9-18, DFAS obtained control and ownership of the DBMS hardware and software responsibilities. Until all functional responsibilities are determined, all parties agreed that the recommendations in this report should be directed to DFAS.

Objective

The overall audit objective was to determine whether the FY 1993 financial statements for the Commissary Operations Fund are presented fairly and in accordance with generally accepted accounting principles. This report addresses the adequacy of internal controls and DBMS operations for accessing personnel and payroll information.

Scope and Methodology

The universe of DeCA employees with access to the DBMS was obtained from DITSO. As of January 31, 1993, the universe consisted of 3,595 employees with access to either DeCA's personnel or payroll subsystems or both subsystems, within the east and west data bases in the DBMS servicing DeCA Headquarters and six continental United States regions. We reviewed data downloaded from DITSO files as of January 31, 1993, of users with access to the personnel and payroll subsystems. We also reviewed who had access to the time, attendance, leave and earnings (TALE), and supervisory certification in the east and west data bases. We reviewed password usage, analyzed password changes, and questioned what could result from unauthorized and undetected access to DBMS.

We interviewed DeCA personnel responsible for inputting personnel and payroll data into the DBMS, as well as DFAS-Columbus Center personnel who were responsible for processing the data. We contacted DITSO personnel responsible for issuing and controlling user identification numbers and passwords. The computer-processed data obtained from DITSO was considered to be reliable at the time that we received and analyzed the data.

Audit Period, Standards, and Locations. We began the audit in October 1992 as part of the Chief Financial Officers Act audit of DeCA's FY 1993 financial statements. This is an ongoing audit scheduled to be completed in June 1994. This portion of the audit was performed in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. Appendix B lists the organizations visited or contacted during this part of the audit.

Internal Controls

Controls Assessed. We evaluated internal controls applicable to compliance with laws, regulations, and procedures for accessing personnel and payroll subsystems of the DBMS.

Internal Control Weaknesses. The audit disclosed material internal control weaknesses as defined by DoD Directive 5010.38 "Internal Management Control Program," April 14, 1987. Controls were not adequate to prohibit unauthorized access to and the ability to add, change, and delete data in the personnel and payroll subsystems. Additionally, controls were not adequate to ensure that Privacy Act data could not be accessed and manipulated by unauthorized personnel. DeCA had not included access to the personnel and

Introduction

payroll subsystems of DBMS in their annual, assurance statements for FY 1992 or 1993, as required by the DoD Internal Management Control Program, because DeCA did not consider personnel and payroll issues a material concern that warranted inclusion in the annual assurance report. All recommendations in this report, if implemented, and the changes made during our audit will correct the weaknesses. No monetary benefits were identified. Appendix A summarizes potential benefits resulting from audit. Copies of this final report will be provided to the senior officials responsible for internal controls within the Office of the Secretary of Defense, DeCA, DFAS, and the Defense Information Systems Agency.

Prior Audits and Other Reviews

The Richmond Detachment of DFAS, Federal Managers' Financial Integrity Act Division, reviewed the payroll subsystem of APCAPS from May 4 to May 22, 1992. In its September 4, 1992, report to DFAS Headquarters, the Detachment concluded that the APCAPS Payroll Subsystem did not conform to the principles, standards, and related requirements of the General Accounting Office, Office of Management and Budget, and DoD. Payroll totals were not in balance with payroll certifications, and the Payroll for Personnel Services Certification did not agree with disbursements.

The report recommended that the DFAS-Columbus Center correct the out of balance conditions, reconcile biweekly pay totals, develop payroll changes in APCAPS, ensure that pay vouchers and certifications are in agreement, validate pay changes prior to input into APCAPS, cancel access to payroll and personnel functions for persons no longer requiring access, assume access codes are canceled when employees transfer, monitor the certification of the TALE listing, ensure that salary payments are based on authorized entitlements, and perform a validity edit of time and attendance transactions. DFAS concurred with all planned actions with corrective actions to be completed by December 31, 1992.

Although DFAS agreed to take corrective action, we noted problems with the issuing and canceling of access codes, as discussed in Part II of the report.

Part II - Finding and Recommendations

Access to Personnel and Payroll Data

Access to personnel and payroll subsystems in the Defense Business Management System data bases was not adequately controlled. The condition occurred because the Defense Commissary Agency and the Defense Information Technology Services Organization had not established adequate internal controls necessary to limit access to the Defense Business Management System subsystems. Additionally, modification was not made to the Defense Business Management System software to allow assignment of passwords only for initial access to the Defense Business Management System. (Effective October 1, 1993, the Defense Finance and Accounting Service obtained responsibility for the Defense Business Management System hardware and software.) Permitting unrestricted access to both subsystems could result in the unauthorized alteration of records, improper payments, payments to fictitious personnel, and access to Privacy Act information.

Background

During the period of our audit, DeCA requested user identification numbers for its employees from DITSO, which issued the numbers and a DBMS password. The password is intended only for initial access to the DBMS. After initial access, users are to assign themselves a user-unique password. DeCA is responsible for determining who should be given access to DBMS and its subsystems, and ensuring that all appropriate automated data processing security safeguards are in place. DITSO was responsible for controlling access to the DBMS through software controls and issuance of passwords. A memorandum of understanding between DeCA and DITSO established each agency's operational and system security responsibilities concerning access to DBMS.

A user identification number and a password are required to access the east and west data bases and the six subsystems of cost accounting, financial management, payroll, personnel, time and attendance, and supervisory certification. Access is obtained by inputting a user identification number, then a password, which should be user-unique, and finally by entering the subsystem acronym. The user identification number and subsystem acronym are readily determined. The password provides control.

A DoD review is underway to consider replacing the current DBMS with another DoD system. However, it should be noted that the conditions included in this report concerning access to the personnel and payroll system currently used by DeCA would be applicable to any subsequent personnel and payroll system used by DeCA.

Controlling Access to the DBMS

DeCA and DITSO did not have adequate internal controls in place to detect or prevent access abuse. In September 1991, DeCA requested that DITSO provide selected employees in the DeCA Headquarters and regional offices with access to both personnel and payroll subsystems in the east and west data bases. The request was made because actions affecting personnel and payroll records were being forwarded from each civilian personnel office to the DeCA Commissary Region liaison offices for input into APCAPS. To perform this liaison function the employees in the liaison office were granted access to input data into the personnel subsystem and the payroll subsystem of APCAPS. DITSO granted access; however, it cautioned DeCA about the need to segregate personnel functions and payroll functions.

As of January 31, 1993, 3,595 DeCA employees had access to the DBMS, with 71 employees having access to both the personnel and payroll functions. Neither DeCA nor DITSO adequately controlled access to the DBMS. A batch of 36 identification numbers that DITSO assigned to DeCA for the west data base did not identify a specific employee, by name, as the user. Additionally, we could not determine who was using the user identification numbers to access DBMS or what passwords were being used because of an insufficient audit trail.

By gaining access to the DeCA personnel subsystem and payroll subsystem an unauthorized user could have created, modified, or deleted Privacy Act data, such as employees' names, social security numbers, financial institutions with savings and checking account numbers, and earnings and leave balances.

Without adequate internal controls the following scenario could occur.

- o The initially issued password could be used by any of the 3,595 DeCA employees in conjunction with the sequentially numbered user identification numbers to gain access to both the personnel subsystem and payroll subsystem.

- o After access is obtained the unauthorized user could add, change, alter, or delete personnel data and payroll data from any existing employee record if the employee's social security number is known. For instance, an employee could change a pay grade and receive an overpayment.

- o After access is obtained to a personnel subsystem, the unauthorized user could create a fictitious employee record.

- o After creating an employee record the unauthorized user could establish a payroll matrix so that a payroll check would be generated for the fictitious employee. After setting up a fictitious employee record in the personnel subsystem and payroll subsystem the unauthorized user would not need to access DBMS again because the system is designed to automatically pay an employee for 80 hours of work. Entries into DBMS are made only on an exception basis.

Access to Personnel and Payroll Data

o Because a supervisor does not certify the employee record each pay period, the fictitious employee's name will appear on a DFAS list of uncertified employees. Unless specific action is taken, payment will continue because the DBMS software does not have an automatic pay stoppage function.

o Finally, the unauthorized user can remove the fictitious employee from the personnel subsystem and payroll subsystem without question or an audit trail.

At least 71 DeCA employees had authorized access to both the personnel subsystem and the payroll subsystem of the DBMS. Except for seven security personnel, no individual employee should have access to both subsystems. Of the 71 employees, 52 were authorized access to the TALE records. Additionally, 4 of the 52 employees could access both the east and west data bases. Such access afforded employees the opportunity to establish records for and pay a fictitious employee.

Of the 71 employees having authorized access to both the personnel subsystem and payroll subsystem, 16 could access regions other than their own. For example, 16 employees had access to the personnel subsystem and payroll subsystem of the northwest region and the southwest region while assigned to either DeCA Headquarters or the central region. Additionally, in four instances the same user identification number was assigned to more than one employee.

Supervisory and TALE Access

In addition to the 71 employees having access to the personnel and payroll subsystems noted above, 474 employees had access to the payroll subsystem providing them with access to both the employee TALE records and supervisory certification. Employees having either dual or single access included contracting officers, commissary officers, time and attendance clerks, and meat and produce managers. Certain payroll functions such as supervisory certification should be available to supervisors only; and TALE entries should be made available to time and attendance clerks only. Allowing supervisors access to both the supervisory certification and TALE could result in a manipulation of payroll records without detection.

We did not identify any fraudulent overpayments or fictitious employee payments because such identification would require a comprehensive review of personnel and payroll records, which was outside the scope of this audit. However, the lack of controls would make it very difficult for DeCA management to discern such fraudulent activity.

Use of Common Passwords

As of January 31, 1993, of the 3,595 users having access to the DeCA data bases in the DBMS, 1,796 (50 percent) users were still using the initial password issued by DITSO. DITSO provided the same initial password to all DeCA users and those requiring access to DeCA records. Some DITSO-issued passwords had been used for as long as 16 months after receipt.

We could not determine the specific number of employees who have continued to use the DITSO-issued password since October 1991 because employees who are transferred between DeCA's six continental United States regions receive new user identification numbers and the use of the DITSO common password each time they transfer to a new region. Records were not available to indicate whether the transferees changed their passwords. However, for those employees who have not transferred, half continued to use the initial password. We attributed this to inadequate software maintenance at DITSO, which allowed the continued use of the initial password. An audit trail was not available to determine who accessed the DBMS and if they made any unauthorized changes. Software can be written that would lock out users after initial activation of the assigned password, thereby requiring the user to designate a user-unique password.

Recommendations, Management Comments and Audit Response

We recommend that the Director, Defense Commissary Agency and the Director, Defense Finance and Accounting Service jointly:

1. Restrict the number of Defense Commissary Agency (DeCA) employees with authorized access to both the personnel and payroll subsystems and strengthen internal controls to prohibit access by unauthorized personnel.

Management Comments. The Director, DeCA, and the Deputy Director for Business Funds, DFAS, concurred with the recommendation, stating that in October 1993, access by DeCA employees to personnel records in the DBMS was removed, and henceforth DeCA employees' access would be restricted to a single subsystem of DBMS. The complete texts of the managements' comments are in Part IV.

2. Establish a required procedure to periodically match all user identification numbers to active DeCA employees and eliminate batch assignment of identification numbers.

Management Comments. The Director, DeCA, concurred with the recommendation, stating that action was initiated in May 1993, to provide all

Access to Personnel and Payroll Data

DeCA supervisors with a listing annually for verification of the existence of employees and their continued functional requirement to use the DBMS. The annotated listing is to be submitted to the appropriate security office for removal of employees' names from DBMS access, as appropriate.

The Deputy Director for Business Funds, DFAS, also concurred but stated that the standard for DFAS employees called for a quarterly listing of authorized users for supervisor verification and removal, as appropriate.

Audit Response. DeCA's comments are considered responsive, except that we believe the use of a quarterly listing for supervisory verification and removal, as appropriate, would be more effective as an internal control measure. The DFAS comments are also considered responsive.

3. Strengthen internal controls to protect Privacy Act data within the personnel and payroll subsystems.

Management Comments. The Director, DeCA, and the Deputy Director for Business Funds, DFAS, concurred with the recommendation, stating that DeCA's personnel subsystem of the DBMS is no longer accessible to DeCA employees and a separation of duties between the personnel and payroll functions, coupled with the periodic reviews of active DBMS users, provides the needed internal control.

4. Limit user access to only the data base servicing the service center, region, or headquarters where the employees work.

Management Comments. The Director, DeCA, and the Deputy Director for Business Funds, DFAS, concurred with the recommendation. Further, DeCA stated that it had initiated appropriate action in April 1993 to limit a user's access to only the data base servicing the DeCA activity for that user.

5. Program the related software to lock out an employee who does not change the password after initial entry into the personnel and payroll subsystems.

Management Comments. The Director, DeCA, and the Deputy Director for Business Funds, DFAS, concurred with the recommendation. DeCA deferred the necessary corrective action to DITSO. DFAS stated that the DITSO-owned systems, located at the Defense Information Systems Office in Columbus, Ohio, are configured to include an automatic feature to force new users to change the initial password to a user-specified password, the first time a user logs on to the system.

6. Strengthen procedures requiring DeCA employees to periodically change their user passwords to preclude extended use.

Management Comments. The Director, DeCA, and the Deputy Director for Business Funds, DFAS, concurred with the recommendation. DeCA stated that DITSO had initiated a twice-a-year screen message to notify

Access to Personnel and Payroll Data

users of the need to change their passwords by a specified date or the user would be deactivated. DFAS stated that the Defense Information Systems Office will establish a similar control on its sponsored systems that will require a change of passwords every 90 days. This feature will be active on all data bases by the end of April 1994.



Part III - Additional Information

Appendix A. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Type of Benefit
1.	Internal Control. Will limit unauthorized access and prohibit unauthorized access to personnel and payroll subsystems.	Nonmonetary
2.	Internal Control. Will provide a follow-up mechanism for determining legitimate DeCA employees.	Nonmonetary
3.	Internal Control. Will safeguard Privacy Act data.	Nonmonetary
4.	Internal Control. Will limit user access to personnel and payroll subsystems.	Nonmonetary
5.	Internal Control. Will provide increased security for accessing the DBMS.	Nonmonetary
6.	Internal Control. Will provide increased security for accessing the DBMS.	Nonmonetary

Appendix B. Organizations Visited or Contacted

Office of the Secretary of Defense

Assistant Secretary of Defense (Personnel and Readiness), Washington, DC
Assistant to the Secretary of Defense for Public Affairs, Washington, DC
Comptroller of the Department of Defense, Washington, DC

Defense Agencies

Defense Commissary Agency, Headquarters, Fort Lee, Petersburg, VA
Defense Commissary Agency, Central Region Headquarters, Little Creek Naval Amphibious Base, Norfolk, VA
Defense Commissary Agency, Northeast Region Headquarters, Fort Meade, MD
Defense Commissary Agency, Southwest Region Headquarters, El Toro Marine Corps Air Base, Santa Ana, CA
Military District of Washington Central Distribution Center, Cameron Station, Alexandria, VA
Commissary Store, Andrews Air Force Base, Camp Springs, MD
Commissary Store, Annapolis Naval Station, Annapolis, MD
Commissary Store, Bolling Air Force Base, Washington, DC
Commissary Store, Cameron Station, Alexandria, VA
Commissary Store, Eglin Air Force Base, Ft. Walton Beach, FL
Commissary Store, El Toro Marine Corps Air Station, Santa Ana, CA
Commissary Store, Fort Belvoir, Springfield, VA
Commissary Store, Fort Campbell, Louisville, KY
Commissary Store, Fort Monroe, Hampton, VA
Commissary Store, Imperial Beach Naval Air Station, Imperial Beach, CA
Commissary Store, Long Beach Naval Station, Long Beach, CA
Commissary Store, Miramar Naval Air Station, San Diego, CA
Commissary Store, Norfolk Naval Base, Norfolk VA
Commissary Store, Pensacola Naval Air Station, Pensacola, FL
Commissary Store, Quantico Marine Corps Base, Quantico, VA
Defense Electronics Supply Center, Dayton, OH
Defense Finance and Accounting Service - Columbus Center, Columbus, OH
Defense Finance and Accounting Service, Richmond Detachment, Richmond, VA
Defense Information Technology Services Organization, Dayton, OH

Non-Defense Federal Organizations

Department of Transportation, Office of the Inspector General, Washington, DC

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Under Secretary of Defense (Personnel and Readiness)
Assistant to the Secretary of Defense for Public Affairs
Comptroller of the Department of Defense

Department of the Army

Auditor General, Army Audit Agency

Department of the Navy

Auditor General, Naval Audit Service

Department of the Air Force

Auditor General, Air Force Audit Agency

Defense Agencies

Director, Defense Commissary Agency
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Information Technology Services Organization
Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Director, Defense Logistics Information Exchange
Inspector General, Defense Intelligence Agency
Inspector General, National Security Agency

Non-Defense Federal Organizations

Office of Management and Budget
National Security Division Special Projects Branch
U.S. General Accounting Office
National Security and International Affairs Division, Technical Information Center
National Security and International Affairs Division, Defense and National Aeronautics and
Space Administration Management Issues

Non-Defense Federal Organizations (Cont'd)

National Security and International Affairs Division, Military Operations and Capabilities Issues

Chairman and Ranking Minority Member of each of the following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Morale, Welfare and Recreation Panel, Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislative and National Security, Committee on Government Operations

Part IV - Management Comments

Defense Commissary Agency Comments



HEADQUARTERS
ATTENTION OF

DEFENSE COMMISSARY AGENCY
HEADQUARTERS
FORT LEE, VIRGINIA 23801-6300

DEC 7 4 1993

IR

MEMORANDUM FOR INSPECTOR GENERAL, LOGISTICS SUPPORT DIRECTORATE,
400 ARMY NAVY DRIVE, ARLINGTON, VA 22202-2884

SUBJECT: Draft Audit Report on Controls Over Access to Personnel
and Payroll Data for the Defense Commissary Agency
(Project No. 3IA-2002.03)

Reference: DoDIG Memorandum, dtd October 18, 1993, SAB.

Attached are our responses to your recommendations provided by
referenced memorandum. If you have any questions, please contact
Mr. Ben Mikell at (804) 734-8103.

Richard E. Beale, Jr.
RICHARD E. BEALE, JR.
Major General, USA
Director

Attachments:
As Stated

DEFENSE COMMISSARY AGENCY REPLY

SUBJECT: Draft Audit Report on Controls Over Access to Personnel and Payroll Data for the Defense Commissary Agency (Project No. 3LA-2002.03)

Recommendation 1. Restrict the number of Defense Commissary Agency (DeCA) employees with access to both the personnel and payroll subsystems and strengthen internal controls to prohibit access by unauthorized personnel.

Action Taken. Concur. DeCA does not authorize any employee access to both personnel and payroll subsystems. In October, 1993, the Defense Logistics Agency assumed the functional responsibility for entering personnel data for DeCA employees. At that time, the access to personnel records in the Defense Business Management System (DBMS) was removed from DeCA.

Recommendation 2. Establish a required procedure to periodically match all user identification numbers to active DeCA employees and eliminate batch assignment of identification numbers.

Action Taken. Concur. DeCA will send a listing annually through each liaison office to all supervisors for verification of existence of employees who have access to the DBMS. For any person on the list who is no longer a DeCA employee or is still on the list but no longer has a functional requirement to use DBMS, the list will be annotated and submitted to the appropriate security office for removal of employees from the DBMS access. This action was initiated in May 1993.

Recommendation 3. Strengthen internal controls to protect Privacy Act data within the personnel and payroll subsystems.

Action Taken. Concur. The personnel subsystem is no longer accessible to DeCA employees. This function has been transferred to the Defense Logistics Agency. DeCA has taken action to limit access within the payroll subsystem. The requirement to review DBMS users and limit their accesses was issued in a DeCA memorandum on April 7, 1993 and will continue to be conducted on an annual basis.

Recommendation 4. Limit user access to only the data base servicing the service center, region, or headquarters where the employee works.

Action Taken. Concur. DeCA initiated this action as a requirement in the memorandum stated in the response to Recommendation 3.

Recommendation 5. Program the related software to lock out an employee who does not change the password after initial entry into the personnel and payroll subsystems.

Action Taken. DeCA concurs with the recommendation but does not own DBMS; therefore, we are not capable of making changes to the system. The Defense Information Technology Systems Office (DITSO), Dayton, Ohio has the responsibility for changes to DBMS. That office indicated the recommended change will be released shortly.

Recommendation 6. Strengthen procedures requiring DeCA employees to periodically change their user passwords to preclude extended use.

Action Taken. Concur. This action has been effected by DITSO, Dayton, Ohio to be activated twice a year. DITSO notifies users with a screen message that their password must be changed, and provides the date by which this change must occur. If the password is not changed, the user will be deactivated. Software enhancements in DBMS as suggested in recommendation 5 will greatly facilitate this process as it relates to initial passwords. If password aging is included in the software change, regularly scheduled password changes will be more easily controlled as well.

Additional Comments:

Several actions have occurred in the past year to strengthen the operational security of DBMS within the DeCA environment. In March 1993, a DoD Comptroller memorandum sent to the Defense Finance and Accounting Service (DFAS), DITSO, and DeCA addressed many of the same concerns covered in this draft audit report. As a result of this memorandum, DeCA convened a meeting of high level management from each organization to discuss the concerns voiced to the Comptroller by the DoDIG and how best to resolve these issues. DeCA assumed responsibility for issues related to improving DBMS performance within the agency through development and implementation of procedures and by defining duties and responsibilities of key personnel involved in the process. In April, DeCA personnel visited DFAS HQ and the Columbus Center to gain insight on DBMS operation in other organizations. In late March, DeCA directed the mandatory replacement of all generic passwords with unique user generated ones. This was accomplished by memorandums to all organizational levels of DeCA and with on screen messages provided by DITSO, Dayton. This action was followed by a total DeCA wide password change on April 15 using the same methods of notification. Tied to this password change was a review of user access assignments for accuracy and continuing need. DBMS reports were requested, in May, from DITSO depicting user

accesses by DeCA organization. These listings were suspended to organization directors for corrective action. Subsequent to this clean up action another request for reports was initiated to verify corrective actions. To further track the progress of DBMS operation and security issues, DBMS security was included in the DeCA Financial Management Improvement Plan. A policy letter covering DBMS procedures and key duties and responsibilities at all levels is currently in agency wide staffing and is to be published in January.

Concur with internal control weaknesses referenced in Part I of the draft audit report. Automated Information Systems (AIS) security was identified as a material weakness in the DeCA Director's Assurance Statement. The actions highlighted in these comments, however, reflect the positive steps being taken to correct these weaknesses. In addition, the implementation by DFAS, of DBMS software enhancements related to password handling and aging, is critical to the correction of these weaknesses.

Defense Finance and Accounting Service Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

FEB 17 1994

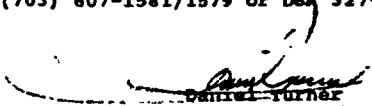
(Business Funds)

MEMORANDUM FOR DIRECTOR, FINANCIAL MANAGEMENT DIRECTORATE
INSPECTOR GENERAL, DOD

SUBJECT: Draft Audit Report on Controls Over Access to Personnel
and Payroll Data for the Defense Commissary Agency
(Project No. 31A-2002.03)

We have reviewed the subject report and attached are
responses to the findings related to the Defense Finance and
Accounting Service.

My point of contact is Mr. Bill deBardelaben. He may be
reached at (703) 607-1581/1579 or DSN 327-1581/1579.


Daniel Turner
Deputy Director for Business Funds

Attachment

Draft Audit Report on Controls Over Access to Personnel and Payroll Data for the Defense Commissary Agency (Project No. 31A-2002.03)

ACCESS TO PERSONNEL AND PAYROLL DATA

- **Recommendation 1:** Restrict the number of Defense Commissary Agency (DeCA) employees with authorized access to both the personnel and payroll subsystems and strengthen internal controls to prohibit access by unauthorized personnel.

DFAS Position: Concur. DeCA has implemented the process to restrict access to a single subsystem of DBMS.

- **Recommendation 2:** Establish a required procedure to periodically match all user identification numbers to active DeCA employees and eliminate batch assignment of identification numbers.

DFAS Position: Concur. This is also a standard for DFAS employees. The DISO Security Office provides a quarterly list of authorized users to the Terminal Area Security Officers (TASOs) who review the listings and delete any user who is no longer an active employee, or who no longer has a need for access to that database/subsystem.

- **Recommendation 3:** Strengthen internal controls to protect Privacy Act data within the personnel and payroll subsystems.

DFAS Position: Concur. The separation of duties between personnel and payroll functions, combined with the quarterly reviews of active user, provides this internal control.

- **Recommendation 4:** Limit user access to only the data base servicing the service center, region, or headquarters where the employee works.

DFAS Position: Concur. While DFAS does not establish which remote users, such as DeCA, may have access to which organization codes, we agree that this is a valid requirement.

- **Recommendation 5:** Program the related software to lock out an employee who does not change the password after the initial entry into the personnel and payroll subsystems.

DFAS Position: Concur. The databases physically located at DISO, Columbus, Ohio are configured so that a new user is forced to change the initial password to a user-specified password the first time that the user logs onto the system.

Attachment

This feature was not installed on the databases physically located at DISO, Dayton, Ohio. However, all DBMS databases are in the process of being relocated to the DISO, Columbus location at which time this feature will automatically be activated. User-specific passwords must be a minimum of six characters in length and a combination of letters and numbers which cannot be easily guessed.

- **Recommendation 6:** Strengthen procedures requiring DeCA employees to periodically change their user passwords to preclude extended use.

DFAS Position: Concur. DISO, Columbus is in the process of establishing an automated system by which user will be required to change their password every 90 days. Some program problems were encountered when an earlier version of this system was installed which delayed implementation on all databases. Current plans call for this feature to be active on all databases by the end of April 1994.

Attachment

Audit Team Members

Shelton R. Young	Director, Logistics Support Directorate
Robert J. Ryan	Audit Program Director
John Yonaitis	Audit Project Manager
Henry Adu	Senior Auditor
Douglas Warish	Senior Auditor
Denise Baldrige	Auditor
Beeson Cho	Auditor
Sheryl Martz	Auditor