Audit Report

OFFICE OF THE INSPECTOR GENERAL

COMPUTER SECURITY OVER THE DEFENSE JOINT MILITARY PAY SYSTEM

Report No. 96-175 June 25, 1996

Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AIS	Automated Information System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DJMS	Defense Joint Military Pay System
DMC	Defense Megacenter
DSE	Directorate of Software Engineering - Military Pay
GAP	Global Access Permission
IG	Inspector General
ISSO	Information System Security Officer
MMPA	Master Military Pay Account
MUTTABLE	Multiple Use Table
OTRAN	Owned Transaction
SLA	Service Level Agreement
TASO	Terminal Area Security Officer
WESTHEM	Western Hemisphere

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

June 25, 1996

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit Report on Computer Security Over the Defense Joint Military Pay System (Report No. 96-175)

We are providing this report for review and comment. This audit was requested by the Director, Defense Finance and Accounting Service, Denver, Colorado. Management comments on a draft of this report were considered in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Based on management's comments, we revised, added, and redirected recommendations in this report to the Defense Finance and Accounting Service and the Defense Information Systems Agency. We request additional comments from the Defense Finance and Accounting Service and the Defense Information Systems Agency on the unresolved, revised, and added recommendations by August 26, 1996. No additional comments are required from the Defense Finance and Accounting Service, Financial Systems Organization, since their comments conformed to the requirements of DoD Directive 7650.3. Specific requirements for additional management comments are stated in Part I of the report.

We appreciate the courtesies extended to our audit staff. Questions on the audit should be directed to Mr. David C. Funk, Audit Program Director, at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Audit Project Manager, at (303) 676-7393 (DSN 926-7393). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 96-175 **June 25, 1996**
(Project No. 5FD-5047)

Computer Security Over the Defense Joint Military Pay System

Executive Summary

Introduction. This audit was requested by the Director, Defense Finance and Accounting Service, Denver, Colorado. The audit focused on the computer security over the payroll application known as the Defense Joint Military Pay System. In FY 1995, this payroll application paid more than $44 billion to active-duty and reserve members of the Army and Air Force. This payroll application was managed by the Defense Finance and Accounting Service centers at Denver, Colorado, and Indianapolis, Indiana. Computer programming support was provided to the two centers by the Directorate of Software Engineering - Military Pay under the Defense Finance and Accounting Service, Financial Systems Organization, Indianapolis, Indiana. The Defense Megacenter, Denver, Colorado, provided computer support to the application.

Audit Objectives. The primary objective was to determine whether application and security software controls adequately safeguarded the data integrity of the Defense Joint Military Pay System. Specifically, we determined whether controls were adequate to limit application access to authorized employees and to limit authorized users to the programs, functions, and data required to perform their duties.

Audit Results. Management and security administrators at the two Defense Finance and Accounting Service centers were very supportive and promptly corrected many problems identified in the security over the Defense Joint Military Pay System.

Opportunities still existed for improving computer security over the Defense Joint Military Pay System. Because of their sensitive nature, the deficiencies discussed in this report are presented in general terms only; specific details of the findings were provided separately to management. Implementing the audit recommendations will eliminate material weakness and strengthen management controls. The results of this audit are summarized below and are detailed in Part I of the report.

o User access at the two centers to the application's master pay datasets, owned transactions, profiles, and the multiple use table was not adequately controlled and limited. Because of these problems, application resources were not secure and the integrity of pay data for active-duty and reserve members of the Army and Air Force was at risk. (Finding A).

o Responsibilities for authorizing and controlling access to the Defense Joint Military Pay System were not clearly defined and understood at one center and two supporting organizations. Accordingly, access to the payroll application and sensitive Army and Air Force pay data was improperly attained, and security oversight was inadequate. (Finding B).

o Administrative controls over application security at the two centers and three supporting organizations needed improvement. As a result, the integrity of the military pay data was vulnerable . (Finding C).

Summary of Recommendations. We recommend that the security administrators at the two centers perform periodic reviews to ensure that user access is being properly controlled and limited. We recommend improvements in defining organizational responsibilities for authorizing and controlling access to the Defense Joint Military Pay System. We also recommend that security administrator positions be established with appropriate authority and oversight capabilities within the two Defense Finance and Accounting Service centers. Also, we recommend that actions be taken at several organizations to identify and control all critical-sensitive positions.

Management Comments and Audit Response. The Defense Information Systems Agency and the Defense Finance and Accounting Service, Financial Systems Organization, concurred with the findings and recommendations. The Defense Finance and Accounting Service concurred with seven recommedations and stated for two other recommendations that it:

o did not take or plan action to elevate the reporting level of the Information System Security Officer at one center.

o would not remove the Global Access Permission attribute from all sensitive profiles. Army field sites used a nonsensitive profile with the Global Access Profile and a restricted (sensitive) profile that does not have the Global Access Permission attribute to correct and release transactions.

We disagreed with the comments on those two recommendations based on industry security standards related to the first recommendation and the lack of justification for management's position on the second recommendation. We ask that the Defense Finance and Accounting Service reconsider its position on those two recommendations.

Based on management's comments, we revised several recommendations and added one in Findings B. and C. to the Defense Finance and Accounting Service, its Financial Systems Organization, and the Defense Information Systems Agency. These changes were made to apply the recommendations beyond FY 1996 and to include another finance center and Defense megacenter as parties to the recommended actions. We also redirected two recommendations in Finding B. to the Defense Information Systems Agency.

See Part I for management comments and our responses, including tables summarizing additional comments required, and Part III for the complete text of management comments. We request additional comments from the Defense Finance and Accounting Service and the Defense Information Systems Agency on the unresolved, revised, and new recommendations by August 26, 1996.

Table of Contents

Part I - Audit Results

Audit Background

The Defense Joint Military Pay System (DJMS) is very large, complex, and by every measure, one of the most sensitive administrative computer applications in the Department of Defense. During FY 1995, DJMS processed over 50 million payroll transactions, valued at $44 billion, for active-duty and reserve members of the Army and the Air Force. The DJMS has also been selected as the migratory pay system for Navy military members. The Naval Academy Midshipmen are currently paid through DJMS with implementation of Navy active-duty and reserve pay scheduled for November 1997. The Directorate of Military Pay at the Defense Finance and Accounting Service (DFAS) Center in Cleveland, Ohio (DFAS Cleveland), was responsible for the Navy active-duty and reserve payroll. The current Navy pay system is installed on mainframe computers operated by the Defense Information Systems Agency (DISA), Western Hemisphere (WESTHEM), Defense Megacenter, Chambersburg, Pennsylvania (DMC-Chambersburg).

The DJMS for Air Force and Army military members is serviced by two DFAS centers. The Directorate of Military Pay at the DFAS center in Indianapolis, Indiana, was responsible for the Army payroll, while the Directorate of Military Pay at the DFAS center in Denver, Colorado, was responsible for the Air Force payroll and the payrolls for all three military academies. For discussion purposes in this report, those two directorates are identified as DFAS Indianapolis and DFAS Denver. Likewise, in this report, the term "Army DJMS" refers to the Army active-duty and reserve components of DJMS. The term "Air Force DJMS" refers to the Air Force active-duty and reserve components of DJMS.

Other organizations also support DJMS. Software development, design, testing, and other central design support for DJMS is provided by the DFAS Financial Systems Organization, Directorate of Software Engineering - Military Pay (DSE) in Indianapolis, Indiana (DFAS DSE Indianapolis) and in Denver, Colorado (DFAS DSE Denver)[1]. The DJMS software was installed on mainframe computers operated by DISA WESTHEM, Defense Megacenter in Denver, Colorado (DMC-Denver). Accordingly, the DMC-Denver is responsible for establishing the means for gaining access to those computers.

The heart of DJMS is a computerized file containing a Master Military Pay Account (MMPA) for every active-duty and reserve member of the Army and Air Force. All data flow into and update the file with output being produced

[1]In January 1996, the Financial Systems Organization realigned managerial authority for military pay systems from the Financial Systems Activity to the Directorate of Software Engineering - Military Pay. This new directorate assumed authority for all Financial Systems Organization resources dedicated to the DJMS and Navy military pay systems. These resources are located in Denver, Colorado; Indianapolis, Indiana; and Cleveland, Ohio.

either from data shown in the file or from daily processing of transactions in the file. The MMPA record contains all information on the member's entitlement, deductions, allotments, collections, payments, status, leave, and payroll history for the past year. All data concerning the member that is, has been, or will be pay determining or relate to any pay distribution are contained in the member's MMPA. As detailed in Appendix A, our audit focused on the controls over individuals that could access or change the MMPAs and other sensitive data.

All MMPAs are maintained by and updated at either DFAS Denver or DFAS Indianapolis. Each center serves as a central site activity for collecting and processing input from several outside organizations, such as the Air Force Finance Services Office and the Army Finance Offices.

DFAS Denver and DFAS Indianapolis used CA-TOP SECRET security software to control access to all DJMS resources, including personnel access capabilities. This security software provided total system security and control over software, data, and data communications. It identified the users allowed access to the computer systems and defined the resources such users were authorized to access. When properly implemented, CA-TOP SECRET security software ensures conformance with DoD security requirements.

Audit Objectives

The objective of our audit was to determine whether application and security software controls adequately safeguarded the data integrity of DJMS. Specifically, we determined whether controls were adequate to limit application access to authorized employees and to limit authorized users to the programs, functions, and data required to perform their duties. In addition, we evaluated the effectiveness of applicable management controls.

See Appendix A for a discussion of the scope and methodology and the results of our review of the management control program.

Finding A. User Access to Application Resources

User access at DFAS Denver and DFAS Indianapolis to DJMS master pay datasets, owned transactions (OTRANs), profiles, and the multiple use table (MUTTABLE) was not adequately controlled and limited. Although some corrective actions were taken, the security administrators need to perform additional reviews of these DJMS resources to adequately limit user access and separate conflicting functions among users. The security administrators at DFAS Denver and DFAS Indianapolis granted access to their respective users without fully evaluating the capabilities allowed or the division of responsibility necessary to separate conflicting functions. Authority and responsibility for granting user access was not fully understood (See Finding B for additional details). In addition, DFAS Indianapolis did not have an Information System Security Officer (ISSO) within their immediate organization (See Finding C for additional details). As a result, DJMS resources were not secure and the integrity of pay data for Army DJMS and Air Force DJMS was in jeopardy. The inadequate controls over user access to these DJMS resources are a material management control weakness.

Master Pay Datasets

At DFAS Denver and DFAS Indianapolis, user access to DJMS master pay datasets was not controlled and limited by the security administrators. These key datasets process the updates to the MMPAs. The security administrators took immediate corrective action to limit user access to the master pay datasets. However, the master pay datasets should be periodically reviewed by the security administrators to ensure that user access continues to be appropriately granted.

Profiles

User access was not adequately controlled and limited for the five sensitive profiles evaluated on the active-duty components of DJMS. The security administrators at DFAS Denver and DFAS Indianapolis immediately took corrective action by removing unnecessary access to some of the sensitive profiles. However, additional reviews were still necessary to further restrict access to authorized users. Each of these sensitive profiles has a collection of access characteristics common to several users and generally describes the access characteristics of a particular job function. For example, a profile may be attached to a user and grants the user access to specific datasets.

The selected sensitive profiles allowed authorized users to perform JDC II and JDC III inputs,[2] quality assurance functions, and the opening and closing of cases by lead technicians and supervisors. These profiles were identified as high risk based on their sensitive capabilities. The profiles were not identically named on the Army active-duty and Air Force active-duty components of DJMS. However, the selected profiles performed the same functions.

At DFAS Denver, reviews were not done to determine whether user access was granted in line with job responsibilities and to ensure that conflicting functions were separated. At DFAS Indianapolis, an ISSO responsible for controlling and monitoring the sensitive profiles had not been appointed within their immediate organization (Finding C). As a result, conflicting functions were not separated for Army active-duty and Air Force active-duty users granted access to these profiles. For example, 422 users for Air Force DJMS and 126 users for Army DJMS could execute the JDC II on-line transaction inputs as well as the JDC II cycle verifications and releases. This access allowed each of those users to control input transactions affecting a military member's pay without supervisory review or oversight.

Global Access Permission

User access to the five sensitive profiles evaluated for the active-duty components of DJMS were not adequately controlled when the Global Access Permission (GAP) attribute was assigned. The GAP attribute was assigned to three of the sensitive profiles evaluated for Air Force active duty and one of the sensitive profiles for Army active duty. When the GAP attribute is assigned to a sensitive profile, the security administrators at the field sites are able to grant access to that profile to any user in their control. This attribute should only be assigned to non-sensitive profiles because of the control weaknesses associated with its assignment to sensitive profiles. Assignment of the GAP attribute was a management decision, not one made by the security administrators. Responsibility for granting user access to these sensitive profiles should be limited to the central site security administrators so access can be controlled to protect the pay data's integrity.

---

[2]Data inputs for Army and Air Force active duty were made using either the JDC II or JDC III subsystem applications. The JDC II and JDC III applications were specifically designed to input active-duty transactions into the daily updates. Inputs were made on-line using JDC II while batch inputs for later file transfer were made using JDC III. Both JDC II and JDC III inputs directly affect the MMPAs.

Owned Transactions

User access was not adequately controlled and limited for the six OTRANs evaluated on the active-duty components of DJMS. The security administrators at DFAS Denver and DFAS Indianapolis immediately took corrective action by removing unnecessary access to some of the high-risk OTRANS. However, additional reviews were still necessary to further limit access to authorized users. These OTRANS are protected as owned resources by the CA-TOP SECRET security software. When a critical transaction is protected as an owned resource, the standard CA-TOP SECRET access rules apply and the owner can limit access to authorized users.

The selected high-risk OTRANs allowed authorized users to perform on-line deletion of erroneous cases, JDC III input file transfers, quality assurance menu functions, JDC II on-line inputs, and deletion of cycles without an audit trail. These OTRANs were identified as high risk based on their sensitive capabilities. The OTRANs were the same on Army active-duty and Air Force active-duty components of DJMS. However, the OTRANs were executed through the use of different profiles.

DFAS Denver and DFAS Indianapolis security administrators granted inappropriate user access to the high-risk OTRANs because they did not clearly understand the capability of each OTRAN. In addition, DFAS Indianapolis did not have within their immediate organization an ISSO responsible for controlling and monitoring access to the OTRANs (Finding C). As a result, conflicting functions were not adequately separated for either Air Force active-duty or Army active-duty users. For example, 27 Customer Information and Control System programmers and production control personnel at DFAS DSE Denver were authorized to execute sensitive OTRANs in both the test and production environments for Air Force DJMS. Likewise, 15 of these programmers and production control personnel at DFAS DSE Denver had access to the test and production environments for Army DJMS. Giving OTRAN users access to both the test and production environments could jeopardize the integrity of the pay data.

Multiple Use Table

Update access to the MUTTABLE datasets was adequately controlled and limited. However, update access to the mainframe dataset for the MUTTABLE on the Air Force active-duty component of DJMS was not adequately controlled and limited. The mainframe dataset had update access granted to 39 DMC-Denver personnel whose job responsibilities in this area were not clearly established. These key datasets process the updates to the MUTTABLE. The MUTTABLE is an important file used to validate DJMS input transactions related to active-duty military members. Once the transactions are validated, they are downloaded to the mainframe dataset. User access to the MUTTABLE datasets and the mainframe dataset had not been periodically reviewed by the

DFAS Denver security administrators. Update capability to the MUTTABLE datasets and the mainframe dataset should be reviewed and verified periodically by the DFAS Denver security administrators to ensure authorized user access.

Recommendations, Management Comments, and Audit Response

A.1. We recommend that the Director, Directorate of Military Pay, Defense Finance and Accounting Service, Denver, Colorado, direct the Information System Security Officers to:

a. Review and verify the need for user access to master pay datasets, sensitive profiles, the multiple use table, and high-risk owned transactions.

b. Review and verify user access to ensure adequate separation of conflicting duties.

c. Remove the Global Access Permission attribute from all sensitive profiles.

Management Comments. Management concurred and stated that all actions were complete. The master pay datasets are now audited and the audit log regularly reviewed. In addition, update capability to the MUTTABLE was changed to READ only capability for selected users. The access profile was reviewed and user access to critical production datasets was changed to READ. Central site profiles were also reviewed and discrepancies corrected to ensure separation of duties. Likewise, the GAP attribute was removed from five sensitive profiles. See Part III for the complete text of management's comments.

Audit Response. Comments were fully responsive to Recommendations A.1.b. and c. For Recommendation A.1.a. actions taken or planned for reviewing and verifying user access to sensitive profiles and high-risk OTRANS were not discussed. We request additional comments in response to the final report.

A.2. We recommend that the Director, Directorate of Military Pay, Defense Finance and Accounting Service, Indianapolis, Indiana, direct the Information System Security Officer, established in accordance with Recommendation C.1.a., to:

a. Review and verify the need for user access to master pay datasets, sensitive profiles, and high-risk owned transactions.

b. Review and verify user access to ensure adequate separation of conflicting duties.

c. Remove the Global Access Permission attribute from all sensitive profiles.

Management Comments. Management concurred with Recommendation A.2.a. and stated reviews of the master pay dataset, sensitive profiles, and high-risk OTRANS were completed on April 11, 1996. Unnecessary user access was removed and measures established to ensure limited access based on individual profile requirements.

Management also concurred with Recommendation A.2.b. and stated review of all Army DJMS users, limited to users within the view capability of the DFAS Indianapolis data base security administrator, was completed on March 21, 1996. User access to profiles that grant conflicting capabilities was restricted. Accordingly, management considered action completed on both recommendations.

Management nonconcurred with Recommendation A.2.c. stating that Army field sites use a nonsensitive profile for correcting transactions and a restricted profile, that does not have the GAP attribute, for releasing transactions.

Audit Response. Management comments were fully responsive to Recommendation A.2.a.

The reviews performed in response to Recommendation A.2.b. were limited to only those users within the security scope of the DFAS Indianapolis data base administrator. We recognize that management cannot perform the required comprehensive reviews of all Army DJMS users until two other recommendations are implemented. First, an ISSO must be established under Recommendation C.1.a. Second, that ISSO must then be given adequate view capability of all Army DJMS users under Recommendation C.2.a. Corrective action is not considered complete until the access capabilities of all Army DJMS users have been reviewed. Additional management comments are requested on this recommendation.

For Recommendation A.2.c., we agree that both nonsensitive and restricted (sensitive) profiles are needed on Army DJMS. There were, however, five sensitive profiles identified during the audit that were assigned the GAP attribute. These sensitive profiles were specifically identified in the technical memorandum that we issued on February 6, 1996, to the Director, Directorate of Military Pay, DFAS Indianapolis. These profiles granted user access to the production region of Army DJMS. In order to achieve centrally controlled access, these five and other sensitive profiles should be restricted. With the GAP attribute assigned to the profile, the security administrators at the field sites can grant access to the profile to any user in their control. When the GAP attribute is assigned, control of sensitive profiles cannot be ensured. We request that management reconsider its comments on this recommendation.

As detailed in the audit response to management's comments on Recommendation B.1.a., the above recommendations may be affected if DJMS security responsibilities are reorganized.

Management Comments Required

Management is requested to comment on the items indicated with an X in the following table.

Table 1. Management Comments Required on Finding A.

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issue
A.1.a.	DFAS		X	X	
A.2.b.	DFAS		X	X	
A.2.c.	DFAS	X	X	X	

Finding B. Organizational Responsibilities

Authority and responsibility for granting and controlling user access to DJMS military pay data were not clearly defined and understood at DFAS Denver, DFAS DSE Denver, and DMC-Denver. This problem occurred because authority and accountability for granting user access to DJMS military pay data were not formally defined. As a result, access was not properly granted or adequately monitored. The inadequate controls over DJMS access were a material weakness in management controls.

Major Areas of Responsibilities

Responsibilities for Army DJMS and Air Force DJMS can be divided into two major areas: software and data. Responsibility for these areas was assigned as described below.

o DJMS software was divided between:

- DFAS Denver, which was responsible for the core software programs that supported DJMS as a whole, and the software specific to Air Force military pay, and

- DFAS Indianapolis, which was responsible for the Army DJMS software bridges and interfaces necessary to interact with the core software, and the software specific to Army military pay.

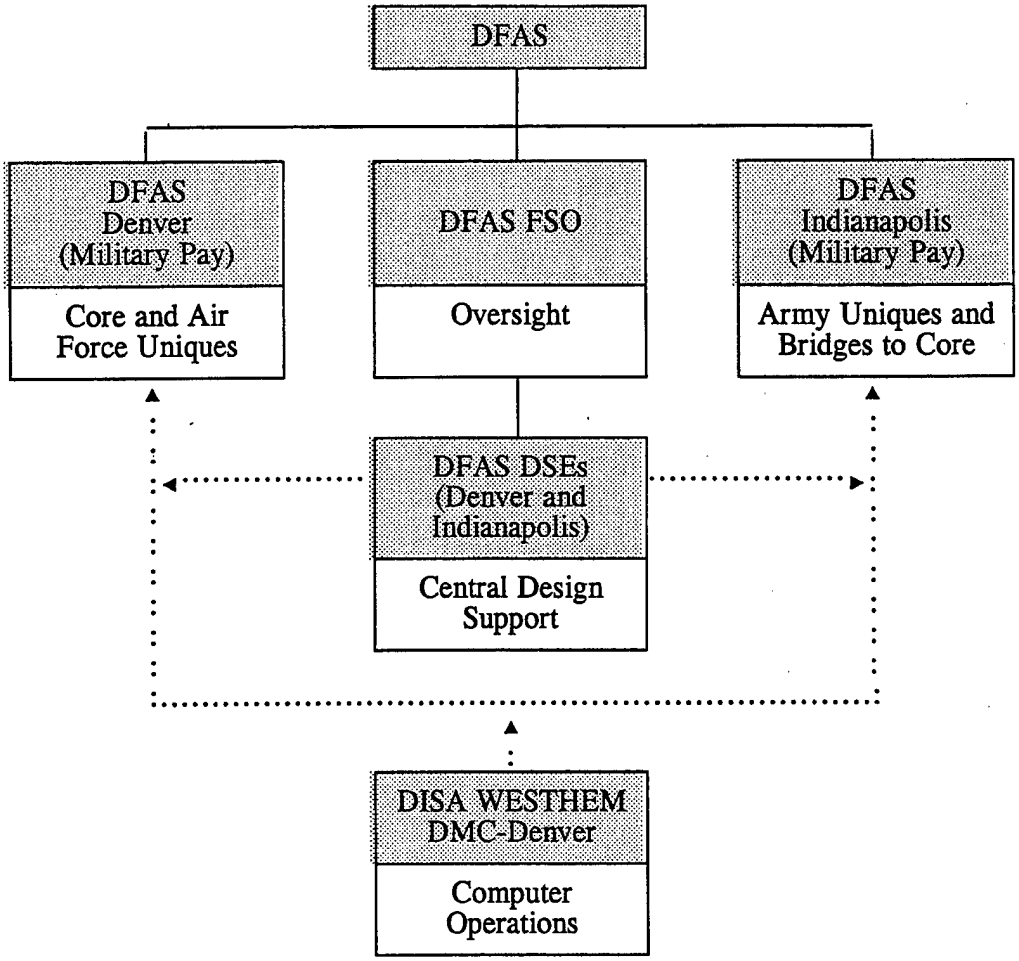
o Similarly, DJMS data was divided between:

- DFAS Denver, which was responsible for the integrity of the Air Force military pay data, and

- DFAS Indianapolis, which was responsible for the integrity of the Army military pay data.

These software and data responsibilities are illustrated in Table 2 by the organizations that manage and support DJMS.

Table 2. Organizations Managing and Supporting the Defense Joint Military Pay System



The DFAS Denver and DFAS Indianapolis were also responsible for authorizing access to the DJMS software and military pay data under its control. Supporting organizations, such as DFAS DSE Denver and DFAS DSE Indianapolis, were required to obtain the approval of DFAS Denver or DFAS Indianapolis, as appropriate, to gain access to the DJMS data. Likewise, if DFAS Denver personnel needed access to the Army DJMS, DFAS Indianapolis had to give its approval (and vice versa). Based on such authorizations, DMC-Denver would then create the user IDs required to gain access to the DJMS application.

System Security

Security Responsibility. The division of security responsibilities between DFAS Denver and DFAS Indianapolis was understood and respected by some personnel within DFAS Denver, DFAS DSE Denver, and DMC-Denver but was misunderstood or ignored by others. This is illustrated by the following examples.

New CA-TOP SECRET Divisions and Departments. Without the knowledge or approval of DFAS Indianapolis, DMC-Denver created new divisions and departments[3] within the CA-TOP SECRET security rules that had access to the Army DJMS database. For example, in March 1995, DMC-Denver created one division with 18 departments having access to the Army DJMS. One of the 18 departments, established by DMC-Denver at the request of DFAS Denver, granted access to six Air Force Accounting Finance Office sites. In addition to not obtaining approval from DFAS Indianapolis for these changes, DMC-Denver did not give DFAS Indianapolis the access required to properly monitor the new division.

Standard User IDs for DFAS Denver Users. User IDs issued by DFAS Indianapolis to DFAS Denver personnel to access the Army database had been deleted and modified by DMC-Denver without the proper coordination with DFAS Indianapolis. DMC-Denver deleted the original user IDs authorized by DFAS Indianapolis and reissued them within the new division described above. As a result of this change, DFAS Indianapolis reported that the access of many of the DFAS Denver users to the Army DJMS was interrupted because the various DJMS tables were not changed to reflect the new IDs. Furthermore, DFAS Indianapolis was unable to assist these users because the DMC-Denver established the new user IDs outside the CA-TOP SECRET scope of the DFAS Indianapolis security administrator (See Finding C for additional details).

New DJMS Profiles. Working with DFAS DSE Denver, DMC-Denver created DJMS profiles and permitted access to DJMS resources without properly notifying DFAS Denver or DFAS Indianapolis (Directorates of Military Pay). During the audit, both DFAS Denver and DFAS Indianapolis issued memorandums to DMC-Denver protesting the creation of these profiles.

DFAS Indianapolis Database Administrator. In one instance, the DMC-Denver refused to provide the database administrator at DFAS Indianapolis with the access required to adequately monitor all user access to the Army DJMS. DFAS Indianapolis requested that its database administrator be given access by DMC-Denver to all CA-TOP SECRET divisions and departments with access capabilities to the Army DJMS. Such access was required by DFAS Indianapolis to properly monitor access to the Army

[3]CA-TOP SECRET uses divisions and departments to establish different levels of access controls.

resources for which it was responsible. The DMC-Denver did not provide the access requested by DFAS Indianapolis because it erroneously believed that DFAS Denver had to approve the request.

Security Accountability. Misunderstandings over DJMS security occurred because the responsibilities and, therefore, the accountability for the integrity of the DJMS software and military pay data were not formally defined and distributed to the organizations involved in maintaining DJMS or in securing the pay data. In January 1995, the DFAS Acting Deputy Director for Information Management agreed with a proposal that DJMS security responsibilities be centralized in DFAS Denver, with the following exception:

> . . . granting of administrative access (e.g., local functional representative's approval of access) to the application should be placed at each operational DFAS Center. The Center operational manager is in the best position to determine access requirements.

Despite this DFAS guidance, in a memorandum to DFAS Indianapolis, DFAS Denver claimed that its security administrators had authority over the Army DJMS. The misunderstandings over DJMS security responsibilities were also shared by DMC-Denver. In responding to security concerns expressed by DFAS Indianapolis, DMC-Denver stated that it was not aware that DFAS Indianapolis should have been notified before it created new security divisions and departments capable of accessing Army DJMS. DMC-Denver referenced the DFAS guidance in its response to concerns expressed by DFAS Indianapolis; however, their actions in this matter were in conflict with that guidance.

Effect on Application Security. Because definitive guidance was not available, DJMS access was not adequately monitored at DFAS Denver and DFAS Indianapolis, and users gained access to DJMS without proper approval. As discussed in Finding A, in many cases, these users did not need the access granted to DJMS to do their jobs. Security personnel at DFAS Indianapolis also did not have the oversight capability required to adequately monitor all Army DJMS users (See Finding C for additional details).

Corrective Actions. On September 25, 1995, the DFAS Deputy Director for Information Management provided the DISA WESTHEM Deputy Chief of Staff for Service Centers with proposed automated information system (AIS) security requirements to be incorporated in the FY 1996 basic service-level agreement (SLA) between the two organizations. These requirements were established by DoD Directive 5200.28, "Security Responsibilities for Automated Information Systems (AIS)," March 21, 1988. This basic SLA, which had not been finalized at the end of the audit, provides the framework for supplemental agreements between each Defense megacenter and the DFAS customers it supports. The SLAs should document each organization's role in providing security to DFAS applications, support systems, and connecting infrastructure. Incorporating these security requirements in the basic SLAs between DFAS and DISA WESTHEM and the supplementary agreements between each Defense

megacenter and its DFAS customers should help prevent future misunderstandings over each organization's role and authority.

Navy DJMS Migration. In February 1996, we briefed the DFAS Assistant Deputy Director for Civilian and Military Pay on the issues discussed in our draft report. The Assistant Deputy Director expressed his support for the findings and recommendations and his intent to apply the recommendations addressed to Air Force and Army military pay to Navy military pay as well. The migration of Navy military active-duty and reserve pay to DJMS is scheduled to be completed by November 1997. As discussed below, the recommendations in this finding directed to DFAS were revised to include DFAS Cleveland. In addition, a recommendation addressed to DISA was added to include DMC-Chambersburg. DMC-Chambersburg provided computer mainframe support for Navy military pay at DFAS Cleveland.

Recommendations, Management Comments, and Audit Response

Revised and Added Recommendations. Based on management's comments, we revised draft Recommendations B.1.a. and B.2.b. to DFAS to include DFAS Cleveland as a party to the memorandum of agreement and supplementary SLAs. Likewise, we added Recommendation B.3.c. to DISA to require that AIS security requirements be incorporated in the SLA between DFAS Cleveland and DMC-Chambersburg. In addition, we revised draft Recommendations B.2.a. to DFAS and B.3.a. to DISA to clarify the need for incorporating AIS security requirements in all future SLAs with one another, not just FY 1996. Finally, because of functional changes in DISA, we redirected Recommendations B.3.a. and b., to DISA. In responding to this report, we request that DFAS comment on revised Recommendations B.2.a. and b. and DISA comment on the new Recommendation B.3.c. As stated below in the audit response to management's comments, additional comments are not required from DFAS on revised Recommendations B.1.a. or from DISA on revised or redirected Recommendations B.3.a. and b.

B.1. We recommend that the Director, Defense Finance and Accounting Service:

a. Develop a memorandum of agreement between the Defense Finance and Accounting Service Centers in Denver, Colorado, Cleveland, Ohio, and Indianapolis, Indiana, and the Financial Systems Organization in Indianapolis, Indiana, that clearly states each organization's authority and responsibilities for defining, controlling, and monitoring user access to the Defense Joint Military Pay System.

b. Disseminate the memorandum to all Defense Finance and Accounting Service, Defense Information Systems Agency, and other organizations involved in securing or maintaining the Defense Joint Military Pay System.

Management Comments. Management concurred with Recommendations B.1.a. and b. stating an agreement is being formulated to clearly state the authority and responsibility for defining, controlling, and monitoring user access to DJMS software and the Air Force, Army, and Navy military pay data bases. One proposal being considered would centralize authority and responsibilities for DJMS security at DFAS Denver. The final agreement must be approved by DFAS and will be distributed to all affected organizations. The estimated completion date is July 31, 1996. See Part III for the complete text of management's comments.

Audit Response. The comments were fully responsive. Although Recommendation B.1.a. was revised to include DFAS Cleveland, management's comments on the draft report indicate that security authority for Navy military pay was considered and will be included in the memorandum of agreement. Therefore, additional comments on the revised Recommendation B.1.a. are not required.

It is important to note that the recommendations made in this report were based on the DJMS security structure in place at the time of the audit. If the security structure for DJMS is reorganized in response to Recommendation B.1.a., several recommendations made in this report could be affected. For example, if DJMS security is centralized at DFAS Denver, an ISSO position may not be required at DFAS Indianapolis in response to Recommendations C.1.a. and b.

B.2. We recommend that the Director, Defense Finance and Accounting Service:

a. Incorporate automated information system security requirements specified by DoD Directive 5200.28 in the service-level agreement with the Defense Information Systems Agency, Western Hemisphere.

b. Direct the Directors of the Defense Finance and Accounting Service Centers in Denver, Colorado; Cleveland, Ohio; and Indianapolis, Indiana, to incorporate the automated information system security requirements specified by DoD Directive 5200.28 in their supplementary service-level agreements with their respective Defense megacenter.

Management Comments. Management concurred, stating that the memorandum of agreement planned in response to Recommendation B.1.a. will incorporate the AIS security requirements. The estimated completion date is July 31, 1996.

Audit Response. Management's proposed alternative does not adequately address Recommendations B.2.a. and b. Incorporating AIS security requirements in the memorandum of agreement on DJMS security, developed under Recommendation B.1.a., is not a viable alternative to the recommended action. The SLAs between DFAS and DISA, which were the recommended vehicle for incorporating AIS security requirements, represent formal contracts for the delivery of specific AIS security services and other computer support between the DFAS centers and Defense megacenters. The memorandum of agreement developed under Recommendation B.1.a. will serve only to clearly

define organizational authority and responsibilities for DJMS security. Including the AIS security requirements in the SLA provides a better means of providing definitive AIS security requirements specified by DoD Directive 5200.28. Additional comments are requested on these recommendations.

B.3. We recommend that the Director, Defense Information Systems Agency:

a. Incorporate automated information system security requirements specified by DoD Directive 5200.28 in the service-level agreements between the Defense Information Systems Agency, Western Hemisphere, and the Defense Finance and Accounting Service.

b. Direct the Director of the Defense Megacenter, Denver, Colorado, to incorporate the automated information system security requirements specified by DoD Directive 5200.28 in the supplementary service-level agreements with the Defense Finance and Accounting Service Centers in Denver, Colorado, and Indianapolis, Indiana.

c. Direct the Director of the Defense Megacenter, Chambersburg, Pennsylvania, to incorporate the automated information system security requirements specified by DoD Directive 5200.28 in the supplementary service-level agreements with the Defense Finance and Accounting Service Center in Cleveland, Ohio.

Management Comments. Management concurred with Recommendations B.3.a. and b. Comments were not provided on the new Recommendation B.3.c. The AIS security requirements were incorporated into the FY 1996 SLA. Likewise, AIS requirements were developed for use in the security portion of the Interservice Agreements between the Defense megacenters and their host installations. In addition, DFAS provided DISA WESTHEM with proposed AIS security requirements for the FY 1996 basic SLAs between DFAS Denver and DFAS Indianapolis. The FY 1996 SLAs are expected to be signed in June 1996. For FY 1997, individual appendixes for individual customers will be developed to incorporate AIS security requirements for each customer. See Part III for the complete text of management's comments.

Audit Response. Management comments were fully responsive. Recommendation B.3.a. was revised to expand its coverage beyond FY 1996. However, management's comments indicated that they already intend to do so by including AIS security requirements in the FY 1997 SLAs. Therefore, additional comments are not required on the revised Recommendation B.3.a. Additional management comments are requested on the new Recommendation B.3.c.

Management Comments Required

Management is requested to comment on the items indicated with an X in the following table.

Table 3. Management Comments Required on Finding B.

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issue
B.2.a.	DFAS	X	X	X	
B.2.b.	DFAS	X	X	X	
B.3.c.	DISA	X	X	X	

Finding C. Administrative Controls Over Security

Administrative controls over DJMS security at DFAS Denver, DFAS Indianapolis, DFAS DSE Denver, DFAS DSE Indianapolis, and the DMC-Denver needed improvement as follows:

o At DFAS Indianapolis, user access on Army DJMS was not adequately controlled because an Information System Security Officer (ISSO) had not been established within the organization.

o The ISSOs at DFAS Denver did not have the level of authority to effectively control DJMS security because of their placement in the organization.

o Requirements for critical-sensitive positions were not met at DFAS Denver, DMC-Denver, and the DFAS DSEs at Denver and Indianapolis for several reasons, including managements' unfamiliarity with certain security criteria and reliance on inaccurate information.

As a result, the integrity of the DJMS pay data was vulnerable. In addition, the security exposure caused by the absence of an ISSO at DFAS Indianapolis was a material management control weakness.

Security Administration

The Directors of Military Pay at the two DFAS centers were responsible for the integrity of the DJMS pay data. The authority to implement and enforce security may be delegated to appointed security administrators. There can be several types of security administrators with varying degrees of authority, such as an ISSO or a Terminal Area Security Officer (TASO). The ISSO is responsible for verifying that security is provided and implemented for the information system, including restricting the use of the computer system resources to authorized individuals and limiting those individuals to using only the resources required to do their jobs. A TASO reports to the ISSO and is responsible for verifying that security is provided for terminals and users in their designated area. The security administrator plays a vital role in safeguarding the integrity of DJMS pay data.

Security Control and Oversight

DFAS Indianapolis did not adequately control and monitor access for all users on Army DJMS. DFAS Indianapolis did not have a security administrator, such

as an ISSO, in their immediate organization with the oversight capability to view, control, and monitor access for all users on Army DJMS. The functions typically accomplished by an ISSO, a critical-sensitive position according to guidelines established by DoD Regulation 5200.2-R, "Personnel Security Program," January 1987, were performed by an individual assigned to the Indianapolis Detachment of DMC-Denver. Consequently, the ISSO was not accountable to the Director of Military Pay.

A security administrator generally has authority over resources and users that fall under his/her functional area of administration. CA-TOP SECRET divides the authority according to the department, division, zone, or the entire installation. The DFAS Indianapolis security administrator, a TASO, had authority over a zone and could only view and monitor the users within the scope of that zone. However, some personnel with access to Army DJMS were outside of this zone and, therefore, were not subject to the control of the TASO. For example, 71 personnel at DMC-Denver, DFAS DSE Denver and DFAS DSE Indianapolis, all of whom had sensitive, high-level access to Army DJMS datasets, were outside of the designated zone. Consequently, though responsible for controlling access to Army DJMS, DFAS Indianapolis did not have the capability required to do so.

Because of this control weakness, the Director of Military Pay at Indianapolis had no assurance that the integrity of the Army pay data was adequately secured. An ISSO should be appointed within DFAS Indianapolis with the authority and capability to enforce security policies and safeguards on all personnel having access to Army DJMS.

Information System Security Officer

The ISSOs at DFAS Denver did not have the level of authority necessary to effectively control DJMS security. The ISSOs for Air Force DJMS did not report directly to the Director of Military Pay at Denver. Instead, the ISSOs reported two levels of management below the Director. To enable the security function to meet overall security objectives and to promote operational independence from user departments, the ISSOs should be placed at a position in the organizational hierarchy that reflects the authority needed. The existing organizational alignment was established to comply with objectives for supervisor-to-employee ratios. This alignment prevented the ISSOs from having the perceived authority within DFAS Denver that would allow them to effectively execute their responsibilities for controlling DJMS access according to DoD Directive 5200.28, "Security Responsibilities for Automated Information Systems (AIS)," March 21, 1988.

Critical-Sensitive Positions

Inadequate security controls existed over individuals with sensitive access to DJMS software and pay data. The DFAS Denver, DFAS DSE Denver, DFAS DSE Indianapolis, and DMC-Denver did not fully comply with one or more of the following requirements in DoD Regulation 5200.2-R.

o Positions should be classified as critical-sensitive if they give individuals access to computer systems that could be used to cause grave damage to the application or data during its operation or maintenance.

o Prior to their appointment, background investigations should be completed on employees who will occupy critical-sensitive positions.

o A waiver must be obtained from the designated official if the delay in appointing someone to a critical-sensitive position without a completed background investigation would be harmful to national security.

Security Controls. Details on these security control weaknesses are provided below.

Position Classifications. At DFAS DSE Denver and DFAS DSE Indianapolis, 41 system programmer positions had not been appropriately classified as critical-sensitive. The same was true for the three ISSO positions at DFAS Denver. A prior audit at the DFAS Financial Systems Activity in Pensacola disclosed similar conditions (Appendix B). These positions were improperly classified for a number of reasons. At DFAS DSE Denver, only personnel with the ability to directly update the MMPAs were classified as critical-sensitive. However, certain programmers at that organization could execute transactions that could also affect the MMPAs. At DFAS DSE Indianapolis, only supervisory positions were classified as critical-sensitive. In addition, DFAS DSE Indianapolis also relied on a DFAS security site review in 1994 that incorrectly reported that all individuals had the required clearances and sensitivity levels. At DFAS Denver, management relied on the Human Resources Directorate rather than themselves to determine the appropriate sensitivity rating for their employees. Also, DFAS Denver did not consider the ISSO positions to be critical-sensitive because they relied on DMC-Denver to provide oversight of their security function.

Background Investigations. DMC-Denver had not requested the required background investigations on three employees and one contractor employee occupying critical-sensitive positions. However, based on prior audits, DMC-Denver was aware that background investigations were required

on two of the four individuals. Similar problems have been identified at other DISA WESTHEM organizations (Appendix B). In response to a recommendation made in Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992, DMC-Denver classified all of its system programmer positions as critical-sensitive. However, DMC-Denver did not verify that background investigations were requested on all personnel assigned to these positions.

Interim Waivers. Pending completion of required background investigations, interim waivers were not obtained for 28 critical-sensitive personnel at DFAS DSE Denver. The waivers were not obtained because management at their parent organization, the DFAS Financial Systems Organization, was not aware that waivers were required.

Personal Integrity of Employees. Meeting the requirements of DoD Regulation 5200.2-R is important to maintaining DJMS security. Personnel in critical-sensitive positions have a high level of access to DJMS resources and, therefore, are not easily subject to management oversight and control. The personal integrity of such employees is an important control. Without the critical-sensitive designation and related background investigation, management has less assurance that personnel placed in positions with considerable access capability are fully worthy of public trust.

Corrective Actions. When management at DFAS Denver was notified of the conditions affecting their personnel, they took immediate corrective action to upgrade the ISSO positions to critical-sensitive. Management at DFAS DSE Indianapolis took partial corrective action by removing sensitive DJMS access for 20 personnel. Management at the DFAS Financial Systems Organization also took partial corrective action by issuing waivers for all personnel already assigned to critical-sensitive positions. However, additional positions were identified that should be classified as critical-sensitive.

Recommendations, Management Comments, and Audit Response

Revised Recommendations. Based on organizational changes, we revised draft Recommendations C.4.a. and b. to apply them to the Director, DFAS Financial Systems Organization DSE. Additional comments are not required on these revised recommendations.

C.1. We recommend that the Director, Directorate of Military Pay, Defense Finance and Accounting Service, Indianapolis, Indiana:

a. Establish an Information System Security Officer position within the Directorate of Military Pay that reports directly to the Director of Military Pay and make that Information System Security Officer responsible for monitoring system access of all users.

b. Designate the Information System Security Officer position as critical-sensitive in accordance with DoD Regulation 5200.2-R.

Management Comments. DFAS concurred with Recommendation C.1.a. stating that an ISSO job description had been completed and submitted for approval and that the ISSO position was designated as critical-sensitive. See Part III for the complete text of management's comments.

Audit Response. DFAS did not comment on whether the ISSO position would report directly to the Director of Military Pay. In addition, no estimated completion date was provided. Additional comments are requested from DFAS on Recommendation C.1.a. Additional comments are not required on Recommendation C.1.b.

As detailed in the audit response to management's comments on Recommendation B.1.a., this recommendation may be affected if DJMS security responsibilities are reorganized.

C.2. We recommend that the Director, Defense Megacenter, Denver, Colorado:

a. Grant the Information System Security Officer (established under Recommendation C.1.a.) at the Directorate of Military Pay, Defense Finance and Accounting Service, Indianapolis, Indiana, with the capability to view all users with access to the Army Defense Joint Military Pay System.

b. Obtain background investigations (and where appropriate, interim waivers) on all current personnel in critical-sensitive positions and before appointing any new individual to such a position, as required by DoD Regulation 5200.2-R.

Management Comments. DISA concurred with Recommendations C.2.a. and b. DISA will provide access to the designated ISSO once DFAS determines which center(s) will have DJMS security authority (Recommendation B.1.a.) and provides guidance to DISA. At that time, DISA will provide an estimated completion date on Recommendation C.2.a. As of February 22, 1996, background investigations or interim waivers had been obtained for all personnel assigned to a critical-sensitive position. In addition, DISA will monitor such positions to make sure that background investigations or waivers are obtained before appointing a new individual to the position. See Part III for the complete text of management's comments.

C.3. We recommend that the Director, Directorate of Military Pay, Defense Finance and Accounting Service, Denver, Colorado:

a. Realign the directorate so that the Information System Security Officer reports directly to Director of Military Pay.

b. Assume responsibility for designating position sensitivity for all positions created within the Directorate of Military Pay.

c. Verify the accuracy of the sensitivity level assigned to all positions within the Directorate of Military Pay in accordance with DoD Regulation 5200.2-R.

Management Comments. DFAS concurred in principle with Recommendation C.3.a. stating the security team already has direct access to the Director of Military Pay, and no specific issues were addressed in the report "that would cause organizational degradation in the current environment."

DFAS concurred with Recommendation C.3.b. (identified in their comments as Recommendation C.4.b.) stating that the sensitivity of the three ISSO positions was upgraded to critical-sensitive.

DFAS concurred with Recommendation C.3.c. and (identified in their comments as Recommendation C.4.c.) stated: "The remaining positions that required security clearances are being processed by the Defense Investigative Service."

Audit Response. DFAS comments on Recommendation C.3.a. require additional clarifications because it did not take or plan any corrective action or offer an alternative solution. Industry security standards recommend that the security function report to a higher level of management to make them independent of the user departments over whom they are expected to exercise control. Elevating the reporting level of the ISSOs would increase overall DJMS security. We request that DFAS reconsider its position and provide additional comments on this report.

Recommendation C.3.b. was made to require the Director of the Directorate of Military Pay to assume responsibility for designating the position sensitivity of all positions within the directorate. The action taken in upgrading the three ISSO positions to critical-sensitive did not adequately respond to the intent of Recommendation C.3.b. DFAS should provide additional comments on this recommendation stating whether or not the Director will assume responsibility for designating position sensitivity within his directorate.

Comments on Recommendation C.3.c. did not specifically state whether or not the recommended review had been performed to verify the sensitivity level assigned to all positions within the Directorate of Military Pay. Management stated that the remaining positions "that required security clearances" were being processed by the Defense Investigative Service. Based on this comment, we are concerned that management may have misunderstood the requirement for critical-sensitive positions. Though background investigations are required, not all critical-sensitive positions require security clearances. We request that management provide additional comments to clarify the actions taken in response to this recommendation. Those comments should state the actions taken or planned to verify the sensitivity assigned to all positions within the directorate.

C.4. We recommend that the Director, Financial Systems Organization, Defense Finance and Accounting Service, direct the Director, Directorate of Software Engineering - Military Pay, to:

a. Designate all sensitive positions as critical-sensitive in accordance with DoD Regulation 5200.2-R.

b. Obtain background investigations (and where appropriate, interim waivers) on all current personnel in critical-sensitive positions and before appointing any new individual to a critical-sensitive position in accordance with DoD Regulation 5200.2-R.

Management Comments. DFAS FSO concurred stating that all sensitive positions were designated critical-sensitive and interim waivers were obtained for all applicable personnel, pending completion of the background investigations. See Part III for a complete text of management comments.

Management Comments Required

Management is requested to comment on the items indicated with an X in the following table.

Table 4. Management Comments Required on Finding C.

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issue
C.1.a.	DFAS	X	X	X	
C.3.a.	DFAS	X	X	X	
C.3.b.	DFAS	X	X	X	
C.3.c.	DFAS	X	X	X	

Part II - Additional Information

Appendix A. Scope and Methodology

Methodology. We examined the access permitted by the CA-TOP SECRET security software to users who could update the DJMS MMPAs. Specifically, we evaluated:

o The access capabilities of users who could affect the MMPAs for active-duty and reserve members of the Army and Air Force through the master pay datasets,

o Selected sensitive profiles based on the high level of risk they presented to the integrity of the military pay data,

o Selected OTRANs based on the high level of risk they presented to the integrity of the military pay data, and

o The access capabilities of users who could update the MUTTABLE.

We also reviewed management policies and procedures for controlling access to DJMS and determined whether these controls adequately limited authorized users to the programs, functions, and data required to perform their duties.

Audit Scope. Because of the size and complexity of DJMS, the audit scope was narrowly defined to only include evaluating the datasets, profiles, and OTRANS discussed above. We also limited the scope of our audit of the management control program, as discussed below.

In the input submitted to DFAS for the FY 1995 Annual Statement of Assurance, DFAS Denver and DFAS Indianapolis identified three material weaknesses in DJMS management controls that related to our specific audit objectives. Three additional weaknesses were identified in the FY 1995 System Manager/User Review for DJMS. Of the six reported weaknesses, corrective action had been completed on two. We did not follow up on the corrective actions taken on the remaining four open weaknesses since corrective actions were still underway. Because of resource limitations, followup on the two corrected weaknesses was deferred to subsequent audits. The audit of the management control program was limited to evaluating its implementation at DFAS Denver and DFAS Indianapolis.

Use of Statistical Sampling Procedures and Computer-Processed Data. To achieve the audit objectives, we did not rely on statistical sampling procedures. However, we did rely on computer-processed data extracted from the security software database provided by CA-TOP SECRET. To test security rules and features and access authorizations, we used the audit features of that security software. All system testing and use of security software was accomplished in a controlled environment with management's approval. We used automated and manual techniques to analyze system data. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Organizations Visited, Audit Period, and Standards. We performed audit work primarily at DFAS Denver and DFAS Indianapolis, the DMC-Denver, DFAS DSE Denver, and DFAS DSE Indianapolis. This financial-related audit was performed from August 22, 1995, through February 2, 1996. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD, and accordingly included such tests of management controls as were considered necessary. During the audit, we visited or contacted the organizations shown in Appendix C.

Management Control Program

DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Control Program. We evaluated the implementation of the DoD management control program at DFAS Denver and DFAS Indianapolis. Specifically, we evaluated the adequacy of management controls over the security of DJMS and other general controls. We also reviewed the results of any self-evaluation of those management controls.

Adequacy of Management Controls. At DFAS, DFAS Denver, and DFAS Indianapolis, we identified material weaknesses in the management controls at the DFAS level, as defined by DoD Directive 5010.38. Controls over DJMS security did not ensure that:

o User access to DJMS resources was adequately limited and controlled (Finding A),

o Organizational responsibilities were clearly defined and understood (Finding B), and

o Adequate security control and oversight existed over user access to Army DJMS (Finding C).

If implemented, Recommendations A.1.a. through c., and A.2.a. through c., B.1.a. and b., B.2.a. and b., B.3.a. through c., C.1.a. and b., and C.2.a. will improve the security of DJMS. The monetary benefits of making these improvements could not be quantified. A copy of the report will be provided to the senior official responsible for management controls at DFAS, DFAS Denver, and DFAS Indianapolis.

Adequacy of Management's Self-Evaluation. The DJMS security function was not identified as an individual assessable unit at either DFAS Denver or DFAS Indianapolis. At DFAS Denver, the DJMS security function was included as part of the assessable unit for the Business Management Division of

the Directorate of Military Pay, which was assigned a medium risk. At DFAS Indianapolis, the DJMS security function was included as part of the assessable unit for the Operations Center of the Directorate of Military Pay, which was assigned a low risk.

The risk assessments accomplished in FY 1992 were not representative of the changes that had taken place in the organizational structures of the two entities. For example, in FY 1992, the security function at DFAS Denver was under the assessable unit for the Configuration Management Division of the Directorate of Military Pay. In a subsequent reorganization, the DJMS security function moved to the Directorate's Business Management Division, another assessable unit, and the Configuration Management Division was eliminated. New risk assessments were not performed by DFAS Denver after the reorganization, and the risk associated with the DJMS security function was not incorporated into the evaluation for the Business Management Division. If Recommendations C.1.a. and C.3.a. are implemented, the DJMS security function at both centers would report directly to the Directors of the Directorate of Military Pay. Based on the established practices within those two directorates, the DJMS security functions would then be established as individual assessable units. The DJMS security function would be appropriately rated high risk based on the sensitivity of their work and the results of this audit. DFAS Denver and DFAS Indianapolis officials did not identify the specific material management control weaknesses identified by this audit because their evaluations covered a much broader area.

Appendix B. Prior Audits and Other Reviews

No prior audits or other reviews related to our specific audit objectives were made of DJMS within the past 5 years. However, similar to the problems discussed in Part I., Finding C., prior Inspector General (IG), DoD, audits determined that sensitive positions at one DFAS organization and several DISA WESTHEM information processing centers had not been properly designated as critical-sensitive as required by DoD Regulation 5200.2-R. The reports issued on these prior audits and the audit followup made on them are discussed below.

IG, DoD, Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992. The report identified sensitive system programmer and contractor positions that had not been designated as critical-sensitive at the DISA Defense Information Technology Services Organization, Information Processing Centers in Cleveland, Ohio (now DISA WESTHEM Defense Information Processing Center-Cleveland) and Indianapolis, Indiana (now defunct), respectively. Management concurred with the audit recommendation to designate those positions as critical-sensitive. Subsequent audit followup verified that management had taken the necessary corrective action (See IG, DoD, Report No. 95-263, "Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service," June 29, 1995).

IG, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993. The report identified sensitive system programmer positions that had not been designated critical-sensitive at the DISA Defense Information Technology Services Organization, Information Processing Activities in Columbus and Dayton, Ohio. The Columbus organization is now the DISA WESTHEM DMC-Columbus. The Dayton organization no longer exists because its work load migrated to DMC-Columbus during FY 1994. Management concurred with the audit recommendation to designate those positions as critical-sensitive. Subsequent audit followup verified that management had done so (See IG, DoD, Report No. 95-263).

IG, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994. The report identified sensitive system programmer positions that had not been designated critical-sensitive at the DFAS Financial Systems Activity in Pensacola (Florida); the Marine Corps Computer and Telecommunications Activity and its Worldwide Support Division in Quantico, Virginia; and the DISA Defense Information Systems Organization, Defense Information Processing Center, Kansas City, Missouri. Management concurred with the audit recommendations to designate those positions as critical-sensitive and obtain the necessary background investigations. Subsequent audit followup verified that management had initiated corrective action, as detailed in the following reports.

Appendix B. Prior Audits and Other Reviews

o IG, DoD, Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995, reports on the followup made at DFAS Financial Systems Activity in Pensacola (now DISA WESTHEM Defense Information Processing Center-Pensacola).

o IG, DoD, Report No. 96-053, "Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service," January 3, 1996, reports on the followup made at DMC-St. Louis, which was responsible for acting on the recommendations made to the Kansas City and Quantico organizations.

Appendix C. Organizations Visited or Contacted

Department of the Army

Detroit Field Office, Army Audit Agency, Detroit, MI

Other Defense Organizations

Defense Finance and Accounting Service, Arlington, VA
- Defense Joint Military Pay System Program Management Office, Defense Finance and Accounting Service, Cleveland, OH
- Defense Finance and Accounting Service, Denver, CO
- Defense Finance and Accounting Service, Indianapolis, IN
- Financial Systems Organization, Defense Finance and Accounting Service, Indianapolis, IN
- Financial Systems Organization, Directorate of Software Engineering-Military Pay, Denver, Colorado

Defense Information Systems Agency, Arlington, VA
- Inspector General, Arlington, VA
- Defense Megacenter, Denver, CO
- Indianapolis Detachment, Indianapolis, IN

Appendix D. Report Distribution

Office of the Secretary of Defense

Deputy Chief Financial Officer
  Director, Chief Financial Officer Support Office
    Chief, Internal Management Control Division
    Internal Control Officer
Deputy Comptroller (Program/Budget)
Assistant to the Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange
Internal Control Officer, Directorate for Organizational and Management Planning, Administration and Management

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Finance and Accounting Service
  Director, Defense Finance and Accounting Service Cleveland Center
    Director, Directorate of Military Pay
  Director, Defense Finance and Accounting Service Denver Center
    Director, Directorate of Military Pay
  Director, Defense Finance and Accounting Service Indianapolis Center
    Director, Directorate of Military Pay
  Director, Defense Finance and Accounting Service, Financial Systems Organization
    Director, Defense Finance and Accounting Service, Financial Systems Organization, Directorate of Software Engineering

Other Defense Organizations (cont'd)

Program Manager, Defense Joint Military Pay System Program Management Office, Defense Finance and Accounting Service
Audit Control Office, Office of the Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Commander, Center for Information Systems Security
Commander, Defense Information Systems Agency, Western Hemisphere
Director, Defense Megacenter-Denver
Director, Defense Megacenter-Chambersburg
Inspector General, Defense Information Systems Agency
Director, Operations, Operations Requirements, and Customer Support Division
Internal Control Officer, Defense Information Systems Agency, Office of the Comptroller
Assistant Inspector General for Audit, Defense Intelligence Agency Inspector General
Policy Liaison Division, Office of the Assistant Director, Policy and Plans, Defense Contract Audit Agency
Chief, Internal Review Group, Defense Logistics Agency
Inspector General, National Security Agency
Audit and Internal Management Control Liaison, National Security Agency

Non-Defense Federal Organizations and Individuals

Special Projects Branch, National Security Division, National Security and International Affairs, Office of Management and Budget
Information Management and Technology Division, General Accounting Office
Technical Information Center, National Security and International Affairs Division, General Accounting Office
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 National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security

This page was left out of orignial document

Part III - Management Comments

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

MAY 6 1996

DFAS-HQ/S

MEMORANDUM FOR DIRECTOR, INSPECTOR GENERAL

SUBJECT: Preparation of Response to DOD IG Draft Report, "Computer Security Over the Defense Joint Military Pay System" dated February 26, 1996 (Project No. 5FD-5047)

We have reviewed the subject audit. Our comments in response to your recommendations for corrective action for findings A, B and C are provided in the attached document.

My point of contact for this action is Ms. Ethel Matthews, (703) 607-3972 or DSN 327-3972.

R. E. Burke
Robert E. Burke
Deputy Director for
Information Management

Attachment

cc: DFAS-HQ/PA
DFAS-DE/DIB
DFAS-IN/QI

DRAFT AUDIT REPORT OR
COMPUTER SECURITY OVER THE
DEFENSE JOINT MILITARY PAY SYSTEM
PROJECT NUMBER 5FD-5047

Finding A: User Access to Application Resources

DFAS DENVER CENTER

Recommendation A.1.a: Review and verify the need for user access to master pay datasets, sensitive profiles, the multiple use table, and high-risk own transactions.

DFAS Comments: Concur. Master Pay datasets (') are being audited and the audit log is reviewed regularly. Update capability to the Multiple Use Table was changed to "READ" only capability for selected users. All management actions completed, no estimated completion date needed.

Recommendation A.1.b: Review and verify user access to ensure adequate separation of conflicting duties.

DFAS Comments: Concur. The "access" profile (') was reviewed and critical production datasets have been changed to "READ" only access. Reviews of central site profiles (') have been accomplished and discrepancies corrected immediately to ensure separation of duties. All management action completed, no established completion date needed.

Recommendation A.1.c: Remove the Global Access Permission attribute from all sensitive profiles.

DFAS Comments: Concur. The Global Access Permission attribute was removed from the five subject profiles (') on March 2, 1996. The six owned transaction (OTRANS) selected in this review (') were placed under tighter control for central site access. All management action completed, no established completion date needed.

*Deleted sensitive data.

Final Report Reference

DFAS INDIANAPOLIS CENTER

Recommendation A.2.a: Review and verify the need for user access to master pay datasets, sensitive profiles, and high-risk owned transactions.

DFAS Comments: Concur. The data base security administrator completed a review of the master pay dataset, sensitive profiles, and high-risk owned transactions on April 11, 1996, for all Army Defense Finance and Accounting Service - Indianapolis Center (DFAS-IN)users. The result provided reasonable assurance that the data base security administrator had removed all unnecessary access and established measures to ensure limited access based on individual profile requirements. The Information System Security Officer (ISSO) job description clearly defines the responsibilities for administrative and security controls. The ISSO will conduct periodic reviews to ensure user access is properly controlled and appropriately granted.

Recommendation A.2.b: Review and verify user access to ensure adequate separation of conflicting duties.

DFAS Comments: Concur. On March 21, 1996, the data base security administrator reviewed profiles of Army users who had conflicting duties. There were 126 users with transaction input capability and cycle verification and release capability. The security administrator changed profiles so users who had both, to only one profile. This review included all Army Defense Joint Military Pay System (DJMS) users within the DFAS-IN data base security administrator's scope.

Recommendation A.2.c: Remove the Global Access Permission attribute from all sensitive profiles.

DFAS Comments: Non-concur. Army field sites use a nonsensitive Global Access Profile for correcting transactions and a restricted non-Global Access Profile, that does not have the Global Access Permission attribute, for releasing transactions.

Revised Page 14

Finding B: Organization Responsibilities

DFAS DENVER CENTER

Recommendation B.1.a: Develop a memorandum of understanding between the Defense Finance and Accounting Service Centers in

Final Report Reference

Denver, Colorado, and Indianapolis, Indiana, and the Financial Systems Organization in Indianapolis, Indiana, that clearly states each organization's authority and responsibilities for defining, controlling, and monitoring user access to the Defense Joint Military Pay System.

Revised B.1.a. to include DFAS Cleveland

DFAS Comments: Concur. This problem is being corrected by the formulation of a Memorandum of Agreement (MOA). The MOA clearly states each organization's authority and responsibilities for defining, controlling and monitoring user access to the DJMS among DFAS-DE, DFAS-IN, DFAS-CL and the Defense Megacenters (DMCS). Specifically, the MOA identifies the Analysis, Configuration, Facilities and Security Branch, DFAS-DE/FJAA, Security Team as the central point responsible for security of all the DJMS resources. The DMC will oversee and administer security on the mainframe computer. DFAS-DE/FJAA will establish policy and procedures for security of all the DJMS resources. They will control access to the DJMS software and the Air Force military pay database. DFAS-IN AND DFAS-CL will serve in the capacity of Terminal Area Security Administrators responsible for validating user request and resetting the DJMS user Ids for Army and Navy military pay databases respectively. The estimated completion date is July 31, 1996.

DFAS-DE resolution for this recommendation is proposed and the MOA will require DFAS-HQ approval.

Recommendation B.1.b: Disseminate the memorandum to all Defense Finance and Accounting Service, Defense Information Systems Agency, and other organizations involved in securing or maintaining the Defense Joint Military Pay System.

DFAS Comments. Concur. The MOA will be approved by DFAS-HQ and will be distributed to all involved organizations. The estimated completion date is July 31, 1996.

Revised B.2.a. to apply to future yea

Recommendation B.2.a: Incorporate automated information system security requirements specified by DoD Directive 5200.28 in the FY 1996 service-level agreement with the Defense Information Systems Agency, Western Hemisphere.

DFAS Comments. Concur. This problem is being corrected in the MOA in recommendation B.1.a. The estimated completion date is July 31, 1996.

Final Report Reference

Revised B.2.b. to include DFAS Cleveland

Recommendation B.2.b: Direct the Directors of the Defense Finance and Accounting Service Centers in Denver, Colorado, and Indianapolis, Indiana, to incorporate the automated information system security requirements specified by DoD Directive 5200.28 in their supplementary service-level agreement with the Defense Megacenter, Denver, Colorado.

DFAS Comments. Concur. This problem is also addressed in the MOA in recommendation B.1.a. The estimated completion date is July 31, 1996.

Finding C: Administrative Controls Over Security

DFAS INDIANAPOLIS CENTER

Recommendation C.1.a: Establish an Information System Security Officer Position with the Directorate of Military Pay that reports directly to the Director of Military Pay and make the Information System Security Officer responsible for monitoring system access of all users.

DFAS Comments: Concur. An ISSO job description has been completed and submitted March 15, 1996, to the Directorate for Resource Management. The proposed title and grade are, military Pay Financial Systems Analyst, GS 501-12, and the position is designated as critical-sensitive. The ISSO will have the authority and capability for safeguarding and enforcing security policies as well as controlling access to Army DJMS. Background investigations will be conducted on all current and new employees assigned to critical-sensitive positions. The ISSO will also have the capability to review profiles of all users with access to Army DJMS.

DFAS DENVER CENTER

Recommendation C.3.a: Realign the directorate so that the Information System Security Officer reports directly to Director of Military Pay.

DFAS Comments. Concur in principle. All the members of the security team have direct access to the Director of Military Pay for any issues that require his immediate attention. There were no specific findings identified in the audit that would cause organizational degradation in the current configuration. Management action completed, no ECD needed.

Final Report Reference

Recommendation C.4.b: Assume responsibility for designating position sensitivity for all positions created within the Directorate of Military Pay. Actually C.3.b.

DFAS Comments. Concur. The three security positions in DFAS-DE/FJAA were upgraded to critical-sensitive. Management action completed, no ECD needed.

Recommendation C.4.c: Verify the accuracy of the sensitivity level assigned to all positions within the Directorate of Military Pay in accordance with DoD Regulation 5200.2-R. Actually C.3.c.

DFAS Comments. Concur. The remaining positions that required security clearances are being processed by the Defense Investigative Service. Management action completed, no estimated completion date needed.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO:
Inspector General

26 April 96

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Acting Director, Finance and Accounting

SUBJECT: Draft DODIG Audit Report on Computer Security Over the Defense Joint Military Pay System (Project No. 5FD-5047)

Reference: DODIG Report, subject as above, 26 Feb 96

We are providing management comments to the subject draft audit report as per your request. We concur with the recommendations and are enclosing actions taken or planned in response to the recommendations. The point of contact is Ms. Sandra J. Leicht, Audit Liaison, on commercial (703) 607-6316.

1 Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

Final Report Reference

MANAGEMENT COMMENTS TO DRAFT DODIG AUDIT REPORT ON COMPUTER SECURITY OVER THE DEFENSE JOINT MILITARY PAY SYSTEM (PROJECT NO. 5FD-5047)

Recommendation B.3.a: Commander, DISA WESTHEM, incorporate automated information system (AIS) security requirements specified by DOD Directive 5200.28 in the FY 1996 service-level agreement with the Defense Finance and Accounting Service.

Redirected and revised B.3.a. to apply to future years

Comment: Concur. The responsibility for service-level agreements (SLAs) was transferred from DISA WESTHEM to DISA Operations, Operations Requirements and Customer Support Division (D31). On 15 April 1996, DISA WESTHEM provided D31 with proposed AIS language to be incorporated into the security portion of the SLAs with DISA WESTHEM customers. The AIS requirements have been incorporated into the boiler plate SLA verbiage for the FY 1996 SLAs. The D31 anticipates the FY 1996 SLAs to be approved and signed by June 1996. A copy of the proposed requirements are at Enclosure 1. In addition, the WESTHEM Security Division (WE5) provided proposed AIS requirements to be used for the security portion of the Interservice Agreements (ISAs) between the Defense Megacenters and their host installation. A copy of those requirements are at Enclosure 2.

Recommendation B.3.b: Commander, DISA WESTHEM, direct the Director, DMC Denver, to incorporate the AIS security requirements specified by DOD Directive 5200.28 in the supplementary SLA with the DFAS centers in Denver and Indianapolis.

Redirected B.3.b.

Comment: Concur. On 25 September 1995, the DFAS Deputy Director for Information Management provided the DISA WESTHEM Deputy Chief of Staff for Service Centers (WE02) with the proposed AIS security requirements to be incorporated into the FY 1996 basic SLA between DFAS-Denver and DFAS-Indianapolis. Implementation of the AIS security requirements have been incorporated into the SLA boiler plate for FY 1996. It is anticipated that the FY 1996 SLAs will be approved and signed by June 1996. For FY 1997, individual appendices for individual customers are being developed that will incorporate AIS security requirements for each customer. Meetings for the FY 1997 SLAs will begin after the FY 1996 SLAs are signed. In the interim, DMC Denver will incorporate the security requirements for access to DISA DMC Denver AIS resources into the current FY 1996 ISA with DFAS.

Added B.3.c. to include DMC-Chambersburg

Recommendation C.2.a: Director, DMC Denver, grant the Information Systems Security Officer (ISSO) at the Directorate of Military Pay, Defense Finance and Accounting Service, Indianapolis, Indiana, with the capability to view all users with access to the Army Defense Joint Military Pay System.

Comment: Concur. DFAS Headquarters, DFAS-Denver, DFAS-Indianapolis are currently negotiating which center should have the security controlling authority for the DJMS platforms. Until the determination is made, DMC Denver cannot grant any authorities. The DMC is awaiting written results and guidance from DFAS based on the results of the negotiations. Once the issue is resolved, DMC Denver will establish the necessary access that DFAS determines appropriate for their ISSO(s). DISA WESTHEM will provide an estimated completion date once the DFAS negotiations are finalized. We will provide an update within three months on the status of the negotiations.

Recommendation C.2.b: Director, DMC Denver, obtain background investigations (and where appropriate, interim waivers) on all current personnel in critical-sensitive positions and before appointing any new individual to such a position, as required by DOD Regulation 5200.2-R.

Comment: Concur. Actions have been completed since the on-site audit and the issuance of the draft report. As of 22 February 1996, background investigations (or interim waivers) have been obtained for the employees and the contractor occupying critical-sensitive positions. The DMC has ensured, and will continue to monitor, that background investigations or waivers for critical-sensitive positions are properly initiated before appointing new employees into the position(s).

Provider will:

1. certify and accredit the DMC infrastructure (hardware, operating system software and communications) IAW with DoDD 5200.28, Mar 88, Security Requirements for Automated Information Systems. DoDD 5200.28 directs that DoD 5200.28-STD (Orange Book), Dec 85, DoD Standard, Trusted Computer System Evaluation Criteria and DoD Manual 5200.28-M, Jan 73, ADP Security Manual as DoD policy. Copies of the accreditation will be provided to the customers.

2. attempt to maintain a C2 level of trust for all operating systems with the DMC. The DISA DAA will analyze any situations of C2 level of trust that cause prohibitively expensive, unsound technically, r adversely impacts operations and make a accreditation decision on a case-by-case basis. Any deviations from the C2 level of trust will be reported to the customer. DISA will address any customer request for a higher level of trust.

3. provide the following minimum security requirements:

a. Access Controls. An access control will be implemented based required personnel security investigations and/or clearances, need-to-know, and authorization.

b. Accountability. Establish an audit trail which as a minimum will record the identity of the user, time of access, interaction with the system, and identify any attempts to modify, bypass, or negate established security safeguards.

c. Accreditation. Accredit the systems to operate in accordance with a DAA approved set of security safeguards.

d. Administrative Security Controls. Establish a security standard operating procedures manual and a users security guide. Establish the following security management structure within the DMC to provide security protection.

(1) Appoint a full time security manager which deals with information, physical, personnel, industrial, communications and emanations security disciplines. These disciplines are apply to protect the DMC facility, equipment, personnel, and information.

(2) Appoint a full time Information Systems Security Manager (ISSM) who is the central point of management of Information Systems Security for the DMC. This person will develop information systems security procedures to implement DoD policy and customer requirements for the protection of the operating systems and the

information they process.

Enclosure 1

(3) Appoint sufficient Information Systems Security Officers (ISSOs) to maintain system access based on. Review audit reports to determine irregularities and report any such deviations for investigation. The DMC ISSO will implement and maintain security control of the operating systems, and established users security profiles for applications as requested by the customer.

e. Availability. Provide established minimum government resource protection based on the known threat.

4. protect classified information during transmission by NSA approved encryption devices and keying material for the megacenter side of the transmission path or by approved protected distribution systems in accordance with DoDD C-5200.5, Dec 87, Communications Security. The provider will establish cryptonets and act as controlling authority for the keying material short titles for those cryptonets.

5. establish that only personnel with properly authorized personnel security clearance have access to classified information in accordance with DoD 5200.2-R, Jan 87, DoD Personnel Security Program.

6. establish an ADP sensitivity program for all personnel having unescorted access to the facility or access to the operating systems in accordance with DoD 5200.2-R.

7. immediately report all expected or known security incidents to their higher headquarters security element and to the ASSIST team while providing information concerning these security incidents to all affected customers.

The customer will:

1. develop applications that will interface and exchange identification and authentication with the known security products utilized by the provider.

2. develop a test plan for their application, and conduct a test of the security for that application. Provide copies of test plan and test results to the provider on demand.

3. provide a certification statement for each application meets all federal policies, regulations, standards, and identify the trusted level requirements.

4. establish, maintain, and submit a copy to provider a need-to-know approval authority list for each application process for them by the provider.

Enclosure 1

5. establish a personnel security program for their users to ensure that appropriate personnel security investigations and/or clearances have been conducted and favorable adjudicated. This includes providing written verification of personnel security investigations, security clearances if applicable, and need-to-know approval for each user request.

6. Identify user access requirements to the DMC ISSOs. Appoint sufficient security officials (alternate ISSOs or Terminal Area Security Officers (TASOs) to maintain access management for their application and interact with DMC security staff.

7. provide the provider with written identification of classification level, classification authority, and classification guidance if applicable for all classified applications and information
being processed for them by the DMC. Also provide written identification of all sensitive but unclassified application and information being process for them by the DMC.

8. immediately report to the provider any suspected or known security deviations or violations.

Enclosure 1

SUPPORT AGREEMENT

Supplier will:

1. Provide a single integrated physical security operation to the door of the facility that satisfies the local physical security program. Provide physical security surveys/inspections and recommendations IAW appropriate local directives.

2. Provide security, law enforcement and resources protection services IAW local directives. Incorporates receivers resources in installation security plan. Coordinates the day-to-day and emergency security requirements of the receiver and supplier to assure the most effective use.

3. Provide identification media, (badges, identification cards and/or vehicle decals) requirements for movement within the installation.

*4. Administer the Personnel Security Program to include suspending, submitting and monitoring personnel security investigations and adverse.

5. Provide initial and recurring security manager's training on local related security issues.

6. Provide counterintelligence support (threat surveys and briefings, and investigations) .

The receiver will:

1. Assist in the development and implementation of the installation physical security resources protection program. Prepare a local security plan and submit to supplier for inclusion into the installation security plan. Ensure that parent commands requirement are made known to the supplier commander. Comply with the supplier security program established in local directives. Participate in emergency security operations as required.

2. Request support. Comply with the supplier's policies and procedures.

3. Comply with supplier's directives and make known to the supplier the requirements .

4. Be responsible for initiating personnel security actions for assigned personnel IAW with supplier directives. Make known the parent commands requirements to supplier commander.

5. Participate in security manager's training program IAW local directives.

Enclosure 2

6. Comply with supplier's directives.

* Not all installations are willing to provide this service. I know that DMC Jacksonville and DMC St. Louis have to do this for their personnel with there own resources. Please notify this office if that is the case at any additional locations.

Enclosure 2

Defense Finance and Accounting Service, Financial Systems Organization, Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
FINANCIAL SYSTEMS ORGANIZATION
8899 EAST 56TH STREET
INDIANAPOLIS, IN 46249-2801

DFAS-DTI

April 26, 1996

MEMORANDUM FOR INSPECTOR GENERAL, ATTN: DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE

SUBJECT: Audit Report on Computer Security Over the Defense Joint Military Pay System (Project No. 5FD-5047)

The Financial Systems Organization, Defense Finance and Accounting Service, concurs with C.4 of Recommendations for Corrective Action as directed to our organization.

Sensitive positions pertaining to the Defense Joint Military Pay System were reviewed during this audit. Required waivers were signed prior to completion of this audit.

Local policy has been modified to reflect the need for waivers when background investigations are in process but uncompleted. All directors have been informed of required procedures regarding sensitive positions. Periodic surveys of the organization's posture regarding sensitive positions have been mandated.

POC for any questions regarding these actions is Mr. Don Stults, DSN 699-5873, commercial (317) 549-5873, or by electronic mail at dstults@cleveland.dfas.mil.

R. E. Burke

Robert E. Burke
Director

Audit Team Members

This report was prepared by the Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD.

F. Jay Lane
David C. Funk
W. Andy Cooley
Frances E. Cain
Phillip L. Holbrook, Jr.
Donna L. Meroney
Monica L. Noell
Susanne Allen

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Computer Security Over the Defense Joint Military Pay System

B. DATE Report Downloaded From the Internet: 12/20/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 12/20/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.