Audit Report

DEFENSE JOINT MILITARY PAY SYSTEM SECURITY FUNCTIONS
AT DEFENSE FINANCE AND ACCOUNTING SERVICE DENVER

Report No. D-2001-166 August 3, 2001

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

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 to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CICS	Customer Information and Control System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DJMS	Defense Joint Military Pay System
ID	Identification
ISSO	Information System Security Officer
OTRAN	Owned Transaction

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

August 3, 2001

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Audit Report on Defense Joint Military Pay System Security Functions at Defense Finance and Accounting Service Denver (Report No. D-2001-166)

We are providing this report for review and comment. We conducted the audit to follow up on prior Defense Joint Military Pay System audits related to security functions performed at Defense Finance and Accounting Service Denver and evaluate related security controls. We considered management comments on a draft of this report when preparing the final report.

Management comments from the Director for Accounting, Defense Finance and Accounting Service, were not fully responsive. DoD Directive 7650.3 requires that all recommendations be resolved promptly. Therefore, we request that the Defense Finance and Accounting Service reconsider its position on Recommendations 3.b., 3.c., and 3.d. Based on management's comments, we revised one aspect of our finding and the related Recommendation 1.a.(1). Additional comments are requested on revised Recommendation 1.a.(1) and the related Recommendation 1.b. Management comments should be provided by August 27, 2001. Specific requirements for the comments are provided in the Recommendation section of the Finding.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Brian Flynn at (703) 604-9489 (DSN 664-9489) (bflynn@dodig.osd.mil) or Mr. W. Andy Cooley at (303) 676-7393 (DSN 926-7393) (wcooley@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Thomas F. Gimble
Acting
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-166 **August 3, 2001**
(Project No. D2000FG-0052.001)
(Formerly 0FG-2119.01)

Defense Joint Military Pay System Security Functions at Defense Finance and Accounting Service Denver

Executive Summary

Introduction. The Defense Joint Military Pay System paid $19.9 billion in FY 2000 to Air Force members. This audit focused on computer security issues that are the responsibility of organizations located at Defense Finance and Accounting Service Denver. Those security issues were reported in two Inspector General, DoD, reports.

- Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996.
- Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System Reserve Component," August 13, 1997.

This audit supplements Inspector General, DoD, Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," February 15, 2001, which focused on the payroll system's overall general controls.

Objectives. Our audit objective was to determine whether adequate corrective actions were taken in response to prior audits of Defense Joint Military Pay System security functions performed at Defense Finance and Accounting Service Denver and evaluate related security controls. Specifically, we determined whether management adequately responded to recommendations made in Inspector General, DoD, Reports No. 97-203 and 96-175 related to system security functions performed at Denver, Colorado. The review of the management control program, as it related to the overall objective, is reported in Inspector General, DoD, Report No. D-2001-052.

Results. Many positive steps were taken by management to implement prior audit recommendations and otherwise improve the security posture of the payroll system. For example, the payroll system manager established a more independent security structure over the payroll system and quickly corrected many of the security weaknesses identified by this audit. However, additional improvements are required in the system's security to fully implement prior audit recommendations and correct additional problems identified by this audit. Several repeat findings were identified. Information system security officers for the payroll system's Air Force-unique resources did not have the independence required to effectively control security over the military payroll application. Inadequate controls existed over user access to sensitive profiles, owned transactions, datasets, and Customer Information Control System regions. Requirements for critical-sensitive ratings for personnel given access

to payroll system resources were not met. In addition, we identified two previously unreported security problems. Access to critical-sensitive Defense Joint Military Pay System resources was not properly documented or controlled. Information system security officers for the payroll system's Air Force-unique resources did not adequately monitor inactive user identifications. As a result, the Defense Finance and Accounting Service did not have adequate safeguards to limit the risks of potential erroneous payments and unauthorized changes to pay data and system resources. Although no fraud or abuse was detected, management identified and corrected more than $152,000 in erroneous payments made in one instance because of improper system access and the lack of separation between conflicting duties. For details of the audit results, see the Finding section of the report.

Summary of Recommendations. We recommend that the Defense Finance and Accounting Service revise an internal regulation and agreement to specify a chain of command independent from the operational elements of the payroll system and provide minimum training requirements for Information System Security Officers. We recommend improvements in internal controls over user access to the payroll system, including individual responsibilities for requesting, monitoring, and verifying user access. We recommend that core security vacancies not be filled until position descriptions with correct sensitivity ratings are in place.

Management Comments. The Defense Finance and Accounting Service concurred in all but three recommendations. Management nonconcurred with revising an internal regulation to clarify the chain of command for security officers, stating that a prior mediation agreement had resolved that issue. Management nonconcurred in providing training on individual responsibilities for requesting and monitoring user access to Air Force computer resources because of other training already provided and recent revisions to internal guidance on requesting and monitoring access. Management nonconcurred in requiring supervisors to annually attest to compliance with DoD security regulations related to critical-sensitive access to Air Force computer resources, stating that supervisors and human resources review position sensitivity ratings and individual qualifications. A discussion of management comments is in the Finding section of the report, and the complete text is in the Management Comments section.

Audit Response. The Defense Finance and Accounting Service comments are fully responsive, except on Recommendations 1.a.(1)., 3.b., 3.c., and 3.d. Management comments concurring in Recommendation 3.c. did not fully address the required corrective actions in reviewing and validating user access to access requests. In nonconcurring on three recommendations, management comments were nonresponsive. The previous mediation agreement cited by management did not relate to Recommendation 1.a.(1) made on defining the chain of command for security officers. However, we revised that recommendation and the related finding discussion to reiterate a prior audit recommendation and request additional comments on that revised recommendation and a related recommendation. The alternative training and procedural changes proposed to Recommendation 3.b. are not an adequate substitute for the recommended training. Also, in nonconcurring in the annual attestations suggested by Recommendation 3.d., management focused on initial hiring controls but did not consider instances where employees are transferred to critical-sensitive positions for which no approved position description exist. We request the DFAS reconsider its position and provide additional comments to the final report by August 27, 2001.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2

Finding

Security Controls for the Defense Joint Military Pay System 3

Appendixes

A. Audit Process
Scope 16
Methodology 17
B. Prior Coverage 18
C. File Transfer Protocol 24
D. Report Distribution 25

Management Comments

Defense Finance and Accounting Service 27

Background

System Overview. The Defense Joint Military Pay System (DJMS) pays active duty, Reserve, and National Guard personnel, and military academy members of the Army, Navy, and Air Force. In FY 2000, the payroll system paid $19.9 billion to Air Force members. Aside from protecting the integrity of payroll records, guarding access to DJMS is important because of the need to protect the privacy of home addresses and other information maintained in the master military pay records of key military members.

Audit Focus. This audit focused only on the following three Defense Finance and Accounting Service (DFAS) organizations at Denver, Colorado.

- Directorate for DJMS Centralized Systems Management, Military and Civilian Pay Services Denver.
- Directorate for Military Pay—Air Force, Military and Civilian Pay Services Denver (formerly the Directorate for Military Pay, DFAS Denver Center).
- Directorate for Technology Services, Support Services Denver (formerly the Directorate for Software Engineering—Military Pay, DFAS Financial Systems Organization).

This audit supplements Inspector General, DoD, Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," February 15, 2001, which focused on the payroll system's overall general controls.

Security Administration. Before February 2000, the Director for Military Pay—Air Force, the functional application manager, was responsible for the computer security for the DJMS core software[1] that supports DJMS as a whole, Air Force-unique software, and pay data for Air Force members. In February 2000, the Director for DJMS Centralized Systems Management (the DJMS System Manager) assumed responsibility for computer security over DJMS core resources.

The authority to implement and enforce security may be delegated to several types of security positions with different authority, such as an information system security officers (ISSOs) or subordinate Terminal Area Security Officers.

- An ISSO is responsible for verifying that security is provided and implemented for the information system, to include 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.

[1]DJMS core software resources are defined as those application resources that affect DJMS processing regardless of where the application resides or who the application is servicing.

- A Terminal Access Security Officer is responsible for verifying that security is provided for terminals and users in their designated area.

Three ISSOs were responsible for DJMS Air Force-unique security while five individuals (including one ISSO) were responsible for security for DJMS core resources. The eight individuals are collectively referred to in this report as the DJMS Security Administrators.

Objectives

The overall objective was to determine the adequacy of management's corrective actions taken in response to prior audits of DJMS security functions at DFAS Denver and evaluate related security controls. Specifically, we determined whether DFAS management adequately responded to recommendations made in the following two Inspector General, DoD, reports related to system security functions performed at Denver, Colorado.

- Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996.

- Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System Reserve Component," August 13, 1997.

The review of the management control program, as it related to the overall objective, is reported in Inspector General, DoD, Report No. D-2001-052. Appendix A discusses the audit scope and methodology. Appendix B lists prior audits related to the audit objectives and gives details on the recommendations followed up by this audit. Appendix C discusses actions taken by DFAS and Defense Information Systems Agency (DISA) to improve the controls over a file transfer protocol used by the payroll system.

Security Controls for the Defense Joint Military Pay System

Many positive steps were taken by management to implement prior audit recommendations and otherwise improve the security posture of the payroll system. However, improvements are required in DJMS security to fully implement prior audit recommendations and correct internal control problems identified by this audit. Adequate corrective actions were not undertaken for the following previously reported conditions.

- The ISSOs for DJMS Air Force-unique resources did not have the independence needed to effectively control DJMS security because the DFAS information security regulation did not create a security structure that defined the chain of command for ISSOs to preclude their reporting to the operational elements over which they enforced computer security.

- User access to sensitive DJMS datasets, profiles, and owned transactions[2] (OTRANs) was not adequately controlled. Most of the DJMS Security Administrators lacked the required technical expertise and training.

- Users' supervisors and DJMS Security Administrators did not meet requirements for critical-sensitive ratings for employees and contractors given access to DJMS resources. Users' supervisors circumvented internal controls or did not request required security waivers, and DJMS Security Administrators were not adequately trained in their responsibilities.

In addition to those repeat findings, we also identified two other DJMS security problems.

- User access requests for access to critical-sensitive DJMS resources were not properly documented or controlled by users' supervisors and the ISSOs for DJMS Air Force-unique resources because they lacked appropriate training.

- The ISSOs for the DJMS Air Force-unique resources did not monitor inactive user identifications (IDs) to ensure that a continuing need for access existed because they lacked the required technical expertise and training.

As a result, DFAS did not have adequate safeguards to limit the risks of potential erroneous payments and unauthorized changes to pay data and systems resources.

[2]The OTRANs are critical transactions, access to which are controlled by Computer Associates International, Inc., TOP SECRET security software. For example, an OTRAN may allow users to perform on-line deletions and inputs.

ISSO Independence

Prior Audit. Inspector General, DoD, Report No. 96-175 stated that ISSOs responsible for DJMS core and Air Force-unique resources did not have the level of authority to effectively control DJMS security. The ISSOs reported two levels of management below the Director for Military Pay—Air Force. The prior audit recommended that the director realign the directorate so that the ISSOs reported directly to the director (Recommendation C.3.a.). DFAS concurred in principle in the recommendation made in the final report but did not plan to realign the ISSO reporting structure because of their interpretation of DoD Directive 5200.28, "Security Responsibilities for Automated Information Systems (AIS)," March 21, 1988. The Inspector General, DoD, and DFAS mediated the issue, and a mediation agreement was signed on December 24, 1996. The agreement required DFAS to address the audit concerns in a pending internal DJMS memorandum of agreement. However, neither the April 8, 1997, version nor the June 15, 2000, revision to the DJMS memorandum of agreement specified where the DJMS ISSOs would be aligned within their chain of command. The prior recommendation was superceded by recommendations made in a subsequent audit.

Related Audit. The organizational placement of the DJMS ISSOs and other DFAS ISSOs was questioned in Inspector General, DoD, Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999. To provide ISSOs with the level of authority and independence necessary to protect application data, that report recommended that DFAS revise DFAS Regulation 8000.1-R to:

- define the operational elements of each automated information system over which security requirements must be enforced (Recommendation 1.b.(2)), and

- create a security structure within DFAS that defines the chain of command for ISSOs to ensure they do not report to the identified operational elements (Recommendation 1.b.(3)).

In its September 28, 1999, comments on the final report, DFAS changed its position from partially concurring to fully concurring in the two recommendations. However, subsequent revisions made to the DFAS regulation did not fully create a security structure that defines the chain of command for the ISSOs.

DFAS Regulation. DFAS made many positive changes to strengthen computer security in the subsequent revisions it made to DFAS Regulation 8000.1-R, "Information Management (IM) Corporate Policy" (formerly "Information Management Policy and Instructional Guidance"), part G., chapter 1, "DFAS Information Assurance Policy," July 18, 2000.

Operational Element. In concert with Recommendation 1.b.(2) in Inspector General, DoD, Report No. 99-107, DFAS revised DFAS Regulation 8000.1-R to define the operational element as the end-user

population and all Central Design Activity personnel who maintain the system software.

ISSO Chain of Command. Other revisions made by DFAS to the regulation did not create a security structure that clearly defined the chain of command for ISSOs to preclude their reporting to those operational elements, as was agreed to under Recommendation 1.b.(3) in Inspector General, DoD, Report No. 99-107. DFAS Regulation 8000.1-R requires the Information System Security Manager to appoint the ISSO. However, the regulation does not identify the Information System Security Manager or any other official as the direct-line supervisor for the ISSO. The DJMS Information System Security Manager verified that she does not supervise the DJMS ISSOs at DFAS Denver.

Repeat Finding. Until February 2000, security for the DJMS Air Force-unique and core resources was the responsibility of the Director for Military Pay—Air Force. As a result of security problems identified with DJMS core resources, the DJMS System Manager assumed security responsibility for those core resources and established an interim DJMS core security team. Security control over Air Force-unique resources remained the responsibility of the Director for Military Pay—Air Force. The division of DJMS security responsibilities was a positive step that strengthened the independence of DJMS-core security. However, contrary to Recommendation 1.b.(3) made in Inspector General, DoD, Report No.99-107, three ISSOs responsible for DJMS Air Force-unique security did not have the independence necessary to effectively execute their responsibilities under DoD Directive 5200.28. Instead, those three ISSOs were assigned to the Directorate for Military Pay—Air Force, which is part of the operational element (end-user population) over which the ISSOs must enforce computer security. This occurred because DFAS Regulation 8000.1-R did not create a security structure that clearly defined the chain of command for ISSOs to preclude their reporting to those operational elements. The DFAS regulation should be revised to clearly identify the direct-line supervisor over the ISSOs as being the Information System Security Manager or another manager who is not part of the operational element over which the ISSO enforces security, such as the System or Project Manager. Corresponding changes should be made to the DJMS memorandum of agreement.

User Access Controls

Prior Audit. Inspector General, DoD, Report No. 96-175 stated that DJMS Security Administrators did not adequately control user access at DFAS Denver to master pay datasets, sensitive profiles, high-risk owned transactions, and the multiple use table, or ensure proper separation of conflicting duties among users. To correct these problems, the prior audit recommended that user access to these DJMS resources be reevaluated. The DFAS Deputy Director for Information Management concurred, stating that corrective actions had already been completed.

Repeat Finding. User access to DJMS master pay datasets, OTRANs, and profiles was not adequately controlled and limited to users with a valid need for access to DJMS core and Air Force-unique resources. In addition, DJMS

Security Administrators granted conflicting user access to Customer Information Control System (CICS) regions and other DJMS resources.

Datasets. User access to DJMS critical datasets was not adequately controlled and limited by DJMS Security Administrators. Specifically, 58 Defense Megacenter Mechanicsburg operations personnel[3] and 10 DJMS production control personnel could make changes to DJMS datasets. At least 462 individual users could read DJMS Active Component and DJMS Reserve Component source code, which allowed them to identify and possibly take advantage of flaws in the internal control system. In addition, redundant and conflicting security software access rules were written for Reserve Component datasets. Because these datasets process the updates to the master military pay record, they should be properly maintained.

Profiles. User access to profiles was not adequately controlled and limited. For example, proper separation of conflicting duties was not maintained because profiles allowed 58 OTRANs to be changed by DJMS production control personnel[4] and gave central site access to 11 field-level personnel. In addition, 20 nontest personnel had access to DJMS test resources by a system test acceptance profile. Uncontrolled profile access further compromised the integrity of DJMS.

Owned Transactions. User access was not adequately limited and proper separation of conflicting duties was not maintained. Excessive access to five command-level and five DJMS active duty component OTRANs was granted. During this audit, security personnel limited user access to the command-level OTRANs and one of the DJMS active duty component OTRANs. However, five DJMS active duty component OTRANs needed further attention. For example, 169 users had production access to the final separation payroll and 48 users had on-line delete access to production cases.

In addition, proper separation of conflicting duties was not maintained with users having access to OTRANs. A conflict situation existed with 37 users who could both create and release DJMS transactions to the master pay records. Furthermore, user access to the DJMS CICS regions was not adequately controlled to ensure a separation of conflicting duties. For example, 565 users[5] had simultaneous access to the Air Force CICS production region and a test region. Unrestricted access given to DJMS users jeopardizes the integrity of the payroll system. The DJMS Security Administrators need to perform periodic reviews of these DJMS resources to adequately limit user access and ensure proper separation of conflicting duties.

---

[3]The DJMS Security Administrators later removed the access to those datasets granted to Defense megacenter personnel.

[4]The DJMS Security Administrators later removed the access to those datasets granted to DJMS production control staff.

[5]The number of users was reduced from the total reported in a draft of this report.

Technical Expertise and Training. Although responsible for immediately resolving high priority security issues, only one of the eight DJMS Security Administrators possessed the qualifications, technical knowledge, and skills necessary to effectively administer DJMS security. Because most DJMS Security Administrators lacked necessary job skills and training, they improperly relied on the user's supervisor and the Terminal Access Security Officer to request appropriate access for DJMS users. The DJMS Security Administrators did not determine through their own research whether the requested user access was appropriate and required by functional responsibility.

Security Training. In response to a related audit,[6] DFAS Arlington[7] revised DFAS Regulation 8000.1-R to outline specific training requirements for ISSOs and other DFAS security positions in the regulation. (However, the revised DFAS regulation and its DFAS Information Assurance Training and Certification Plan did not establish appropriate training requirements for ISSOs.) Under the DFAS regulation, DJMS and other ISSOs are only required to meet the training requirements for "relatively inexperienced" level 1 system administrators. Paragraph 7.9 of the regulation needs to be revised to require that ISSOs meet the training requirements for level 2 system administrators. Level 2 system administrators are described as "the workhorses in a domain," who perform the majority of daily tasks that keep a domain running smoothly.

Summary. Because DJMS Security Administrators lacked technical training and expertise, DJMS resources were not secure, and the integrity of DJMS pay data was in jeopardy. For example, in December 1999, over $152,000 in erroneous payroll payments were transmitted to the Federal Reserve Bank for payment to members (though later recalled) because test personnel were improperly given access to production resources by the Air Force-unique ISSOs, whose security responsibilities at that time included DJMS core resources. Because of that incident, the DJMS System Manager assumed security responsibilities for DJMS core resources.

The lack of technical expertise and training for most DJMS Security Administrators was a major factor in the problems discussed below related to critical-sensitive access, user access requests, and inactive users.

---

[6]Details are provided in Inspector General, DoD, Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999.

[7]DFAS Arlington is the nomenclature for Headquarters, DFAS.

Critical-Sensitive Ratings

Recommendations were made in two prior DJMS audits to strengthen the controls over access to critical-sensitive resources.

Inspector General, DoD, Report No. 96-175 reported that the position descriptions for the three ISSOs over DJMS Air Force-unique resources had not been properly rated as critical-sensitive. A critical-sensitive rating is required by DoD Regulation 5200.2-R when the position requires access to computer systems that could be used to cause grave damage to the application or data during its operation or maintenance. DFAS concurred in the recommendations that the Director for Military Pay—Air Force assume responsibility for designating position sensitivity for all positions created within the directorate (Recommendation C.3.b.) and verify the accuracy of the sensitivity level assigned to all positions within the directorate in accordance with DoD Regulation 5200.2-R (Recommendation C.3.c.). This prior audit identified similar problems in the Directorate of Technology Services related to critical-sensitive ratings and required waivers, which were subsequently incorporated in the following report.

Inspector General, DoD, Report No. 97-203. This prior audit reported that critical-sensitive positions in the Directorate of Technology Services were not properly rated as critical-sensitive, requests had not been made for required background investigations, and necessary waivers had not been obtained. DoD Regulation 5200.2-R requires complete background investigations on employees who will occupy critical-sensitive positions before their appointment to those positions. To avoid a delay harmful to national security, the appointment may be made before the investigation is completed if a waiver is obtained from the designated official. Corrective action by DFAS Arlington was necessary because of the DFAS-wide pattern of noncompliance with those DoD security requirements.

In accordance with the mediation agreement with the Inspector General, DoD, on May 10, 1999, the DFAS Director provided written assurance that DFAS was in compliance with the Personnel Security Program. The director stated that the sensitivity ratings for position descriptions had been reviewed and validated and appropriate investigations had been conducted or requested. Because this was an ongoing process, the director stated that procedures were in place in DFAS Human Resources and the servicing security offices to continue meeting program requirements.

Repeat Finding. Inadequate security controls existed over individuals with access to critical-sensitive DJMS software and pay data.

Interim DJMS Core Security Team. Two employees on the interim DJMS core security team were transferred from their positions as financial systems specialists, which were rated nonsensitive. At the time of that transfer, no position descriptions had been developed for the positions occupied by those two individuals on the interim DJMS core security team. Because access to critical-sensitive DJMS resources was required, the position descriptions for

those security positions would have required a critical-sensitive rating. The internal controls designed to detect personnel movements in or out of critical-sensitive positions and automatically generate background investigations (and waivers, when appropriate) did not work in this situation. That is, there was no change in position descriptions when those two financial system specialists were transferred because they continued to work under their old position descriptions. DFAS employees should not be transferred to personnel positions when appropriate position descriptions have not been prepared and approved. Such prohibitions are especially important when a change in the sensitivity rating for the old or new position is involved.

DJMS Production Control. Of the nine DJMS production control personnel, four contract employees in DJMS production control were inappropriately granted sensitive system access by the ISSOs for DJMS Air Force-unique resources. Two contractors did not have the required background investigations although investigations for two other contractors were in process. However, no waivers had been obtained. These conditions occurred, in part, because the supervisor over these contract employees did not request waivers when background investigations had not been completed. Supervisors over DJMS users should receive mandatory training in their responsibilities for requesting system access

Corrective Action. Background investigations were initiated for two contractors and waivers written for the four production-control contract employees. In addition, critical-sensitive access previously granted to the two members of the interim DJMS core security team was reevaluated and removed. Subsequent to the audit, the DJMS System Manager stated that all four DJMS core security positions (reduced from five positions) had been rated as critical-sensitive.

In addition to the repeat findings, two other DJMS security weaknesses were identified related to user access requests and inactive users.

User Access Requests

Documentation Controls. User access to DJMS and its application resources is documented and controlled by the DISA Form 41, "System Authorization Access Request." The DFAS Denver Handbook 8000.1, "Information System Security (INFOSEC) Handbook," December 1999, provides the following guidance on the preparation and use of the DISA Form 41.

- At the request of the user's supervisor, the Terminal Area Security Officer prepares the initial DISA Form 41 (and subsequent modifications and deletions) requesting and justifying the user's access to specific DJMS resources.

- After approval by the user's supervisor, the Terminal Area Security Officer forwards the DISA Form 41 for approval to the functional data owner, the security manager, and finally the DJMS ISSO.

- After reviewing and approving the DISA Form 41, the DJMS ISSO provides the system access requested for the user.

The DJMS ISSO should not approve a DISA Form 41 that is incomplete or request access that conflicts with other access already provided to the user. To evaluate those DISA Form 41 controls, the audit focused on the critical-sensitive access granted under 13 user IDs to 10 DJMS production control users.

DJMS Production Control. Access to critical-sensitive DJMS resources by DJMS production control users under 13 user IDs was not properly documented or controlled by the DISA Form 41. For example, no DISA Form 41 was available to document the initial access that was requested and approved for 4 of the 13 user IDs.

Of the 63 DISA Form 41s provided for the 13 user IDs:

- 13 lacked any supervisory justification for the access requested for the user,
- 17 had not been approved by the functional data owner, and
- 7 had not been approved by the DJMS ISSO.

The documentation and control problems occurred because the ISSOs for Air Force-unique resources and the supervisors over DJMS production control users were not adequately trained in their responsibilities in requesting and granting system access using the DISA Form 41. As a result, the ISSOs for Air Force-unique resources granted access to DJMS resources to these production control users without justification or proper authorization. Effective controls over the DISA Form 41 could have identified and prevented the problems previously discussed related to user access controls and critical-sensitive access. Mandatory training of users' supervisors and those ISSOs should improve the effectiveness of this documentation control.

Inactive Users

The ISSOs for DJMS Air Force-unique resources did not adequately monitor user access to DJMS. Specifically, during this audit, 196 DJMS Air Force-unique users had not accessed the system in over 180 days. The Computer Associates International, Inc., TOP SECRET security software used to protect DJMS resources and locally developed retrieval programs could have been used by those ISSOs to generate reports identifying these inactive user IDs. However, the ISSOs did not periodically generate these reports because they lacked the technical expertise and training to extract and perform such user validations. If inactive user IDs are not promptly suspended (and removed, when appropriate), hackers could use those IDs to gain unauthorized access to the system.

Similar problems with inactive user IDs were reported in Inspector General, DoD, Report No. D-2001-052. Under Recommendations 1.f. and 2.c. to that

report, the DISA Area Command Mechanicsburg and DFAS will jointly develop a procedure for reviewing all user identification codes not used within 35 days. Those recommendations and the improvement recommended by this report in the training requirements for DJMS ISSOs should improve controls over inactive user accounts. Therefore, no additional corrective actions are recommended in this report.

Recommendations, Management Comments, and Audit Response

Revised Finding and Recommendation. Based on management's comments, we revised our finding discussion of ISSO independence and the related Recommendation 1.a.(1) to reiterate Recommendation 1.b.(3) made in Inspector General, DoD, Report No. 99-107. Additional comments are provided in the audit response to management comments on the recommendation.

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

a. Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management (IM) Corporate Policy," part G., chapter 1, "DFAS Information Assurance Policy," July 18, 2000, to:

(1) Create a security structure within the Defense Finance and Accounting Service that defines the chain of command for Information System Security Officers to ensure that they do not report to the operational elements over which security requirements must be enforced.

(2) Specifically identify and establish a minimum level 2 training requirement for information system security officers in the discussion of training requirements in paragraph 7.9.

b. Memorandum of Agreement on the Defense Joint Military Pay System, June 15, 2000, in concert with the changes recommended to Defense Finance and Accounting Service Regulation 8000.1-R.

Management Comments. DFAS nonconcurred with the Recommendation 1.a.(1), stating that the mediation agreement on Inspector General, DoD, Report No. 99-107 had resolved the ISSO reporting issue. As a result, DFAS revised DFAS Regulation 8000.1-R to provide autonomy for ISSOs when enforcing requirements over operational elements. Information System Security Managers appoint ISSOs, who cannot be assigned to the end-user population of a system or to a Central Design Activity directly supporting the production system. ISSOs report to the Information System Security Managers on security matters with an advisory provided to the application's system or project manager.

However, DFAS concurred with Recommendations 1.a.(2) and 1.b., stating that the recommended actions will be completed by December 31, 2001, and January 31, 2002, respectively.

Audit Response. Contrary to management comments, the mediation agreement on Inspector General, DoD, Report No. 99-107 did not relate to Recommendation 1.a.(1) on defining an independent chain of command through which ISSOs should report. Instead, that mediation agreement related to another recommendation made in that report to make ISSOs the direct supervisors over certain security administrators. However, based on management's comments, we revised our finding discussion of ISSO independence to reflect the impact of management's concurrence in two related recommendations made in Inspector General, DoD, Report No. 99-107. We also revised our draft report's Recommendation 1.a.(1) to reiterate the agreed to Recommendation 1.b.(3) made in Inspector General, DoD Report No. 99-107, which was not fully implemented by DFAS. We request that management provide additional comments on the revised recommendation, including the related Recommendation 1.b. on the DJMS memorandum of agreement.

2. We recommend that the Director for Defense Joint Military Pay System Centralized Systems Management, Defense Finance and Accounting Service Denver:

a. Direct the information system security officer to:

(1) Review all user permissions and verify that proper separation of conflicting duties is maintained among users and sensitive access to datasets, profiles, owned transactions, and other Defense Joint Military Pay System core resources is granted in accordance with DoD Regulation 5200.2-R, "Personnel Security Program," January 1987.

(2) Annually provide and report upon training given to supervisors and security administrators on their responsibilities in preparing and processing the Defense Information Systems Agency Form 41, "System Authorization Access Request." Annual attendance at such training should be mandatory for all supervisors who request user access to system core resources and for security administrators over the system's core and Air Force-unique resources.

(3) Validate and document all user access to the corresponding Defense Information Systems Agency Form 41, "System Authorization Access Request."

(4) Annually require that supervisors over system users provide written assurance that position descriptions for system users are assigned the proper sensitivity level and that system users (including contractors) with critical-sensitive access to automated information systems have background investigations (and where appropriate, interim waivers pending completion of such investigations), as required by DoD Regulation 5200.2-R.

b. Verify that position descriptions with correct sensitivity ratings are approved for each position before filling current and future vacancies on the system's core security team.

Management Comments. DFAS concurred in all the recommendations. User access for DJMS core resources was reviewed and validated to ensure system access is controlled. In addition, training was provided to DJMS core supervisors and Terminal Area Security Officers on their responsibilities in processing the system authorization requests. Management reviewed and validated core user DISA Form 41s. Supervisors will provide the annual assurance on position sensitivity and required background investigations for system users. Finally, position descriptions were approved for correct sensitivity ratings in the DJMS core security office. All corrective actions will be completed in FY 2001.

3. We recommend that, pending implementation of Recommendation 1.a.(1), the Director, Directorate for Military Pay—Air Force, Defense Finance and Accounting Service Denver, direct the information system security officers to:

a. Review all user permissions and verify that proper separation of conflicting duties is maintained among users and sensitive access to datasets, profiles, owned transactions, and other Defense Joint Military Pay System Air Force-unique resources is granted in accordance with DoD Regulation 5200.2-R.

Management Comments. DFAS concurred, stating that corrective actions will be completed in FY 2001.

b. Attend the annual training required by Recommendation 2.a.(2) and annually provide and report upon training given to supervisors on their responsibilities in preparing and processing the Defense Information Systems Agency Form 41, "System Authorization Access Request." Annual attendance at such training should be mandatory for all supervisors who request user access to Air Force-unique system resources.

Management Comments. DFAS nonconcurred, stating that training was already provided to DFAS Denver users, as is done at other locations. Revised instructions on the DISA Form 41 were issued. Questions can also be e-mailed to the ISSOs for DJMS Air Force-unique resources. DFAS stated that a training course designed for the various locations serviced by the Denver ISSOs would be cumbersome and redundant.

Audit Response. Management's comments are nonresponsive. The annual training cited by DFAS is not an adequate substitute for the recommended DISA Form 41 training. The training already given to all DFAS Denver employees, which focuses on Internet and e-mail policies, is too general and does not address the DISA Form 41. Updating DFAS Denver instructions on the DISA Form 41 is a positive step, but will not ensure that ISSO, Terminal Area Security Officers, and supervisors comply with those instructions. Proper use of the DISA Form 41 is critical to DJMS security because it provides the basis

for granting access to users. When the DISA Form 41 is not properly used, as was determined by this audit, a higher risk exists for erroneous payments and unauthorized changes to pay data and system resources. We request that DFAS reconsider its position and provide additional comments in response to this report.

c. Validate and document all user access to the corresponding Defense Information Systems Agency Form 41, "System Authorization Access Request."

Management Comments. DFAS concurred, stating that DISA Form 41s are reviewed and validated when they are submitted. Other routine reports identify other irregularities for corrective actions. Corrective action was completed October 27, 2000.

Audit Response. The DFAS comments are only partially responsive because they are incomplete. DFAS corrective actions addressed the review and validation accomplished with the receipt of a new or revised DISA Form 41. Additional comments are required to describe the corrective actions taken or planned in reviewing and validating user access to the DISA Form 41s where such access did not change, thus not prompting the submission of a revised DISA Form 41 to the ISSOs. We request that DFAS provide additional comments in response to this report.

d. Annually require that supervisors of system users provide written assurance that position descriptions for system users are assigned the proper sensitivity level and that system users (including contractors) with critical-sensitive access to automated information systems have background investigations (and where appropriate, interim waivers pending completion of such investigations), as required by DoD Regulation 5200.2-R.

Management Comments. DFAS nonconcurred, stating that position descriptions for the ISSOs for DJMS Air Force-unique resources were properly rated as critical-sensitive. Management also stated that supervisors and human resources review position sensitivity ratings and individual qualifications.

Audit Response. DFAS comments are nonresponsive and incomplete with respect to the corrective actions planned or completed related to supervisory attestations on required background investigations or waivers. Management's comments focused on the process for assigning sensitivity ratings to position descriptions. We agree that assigning the proper sensitivity rating to a position description is a significant control when that position description is first created. That control should automatically trigger requests by human resources for background investigations when critical-sensitive positions are filled. However, the control is effective only when the employee remains in the same position. The audit determined that DJMS employees were transferred from nonsensitive to critical-sensitive positions for which no approved position description existed. Such transfers will not automatically trigger requests for background investigations because human resources staff is unaware of any formal change in the employee's position description. Thus, requiring supervisors to annually

attest to the propriety of the position sensitivity ratings for DJMS users is a fail-safe control intended to identify users who may have transferred to positions with different sensitivity ratings.

Management's comments did not address the supervisory attestations on required background investigations or waivers. The audit determined that contract employees with critical-sensitive access did not have required background investigations or waivers. Obtaining background investigations on employees with critical-sensitive access is a crucial control because of the grave damage such employees could do to DJMS resources. We request that DFAS reconsider its position and provide additional comments in response to this report.

4. We recommend that the Director, Human Resources, Defense Finance and Accounting Service Support Services Denver, establish procedures to periodically alert site supervisors to the importance of and requirement that appropriate position descriptions be established for all personnel positions before filling such vacancies by promotion or reassignment.

Management Comments. DFAS concurred, stating that a memo was sent to all directors, advising that appropriate position descriptions must be established for all positions before filling vacancies. Similar alerts will be provided at the beginning of each calendar year.

Appendix A. Audit Process

Scope

Work Performed. We evaluated the controls over organizational placement of the ISSOs, user access to the DJMS application resources, sensitivity ratings of personnel with sensitive access to DJMS application resources, user access requests, and inactive users. To test security rules and access authorizations, we used the audit features of the Computer Associates International, Inc., TOP SECRET security software.

Limitations to Audit Scope. The review of the management control program, as it related to the overall audit objective, is reported in Inspector General, DoD, Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," February 15, 2001.

DoD-Wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate-level goals, subordinate performance goals, and performance measures. Although the Secretary of Defense has not established any goals for Information Assurance, the General Accounting Office lists it as a high risk area. This report pertains to Information Assurance as well as achievement of the following goal, subordinate performance goal, and performance measures.

- **FY 2001 Corporate-level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-2)**

- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

- **FY 2001 Performance Measure 2.5.1:** Reduce the number of noncompliant finance and accounting systems. **(01-DoD-2.5.1)**

- **FY 2001 Performance Measure 2.5.3:** Qualitative assessment of reforming information technology management. **(01-DoD-2.5.3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

- **Financial Management Functional Area. Objective:** Strengthen internal controls. **Goals:** Improve compliance with the Federal Managers' Financial Integrity Act. **(FM-5.3)**

- **Information Technology Management Functional Area. Objective:** Ensure that vital DoD information resources are secure and protected. **Goal:** Assess the information assurance posture of DoD operational systems. **(ITM-4.4)**

General Accounting Office High Risk Area. The General Accounting Office has identified several high risk areas in the DoD. This report provides coverage of the Information Security and Defense Financial Management high risk areas.

Methodology

Use of Computer-Processed Data. We relied on computer-processed data extracted from the security software database provided by Computer Associates International, Inc., TOP SECRET security software for DJMS. All systems testing and use of security software audit tools were accomplished in a controlled environment with management 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.

Audit Type, Dates, and Standards. This financial-related audit was performed from March 2000 through March 2001. We did our work in accordance with generally accepted Government auditing standards except that we were unable to obtain an opinion on our system of quality control. The most recent external quality control review was withdrawn on March 15, 2001, and we will undergo a new review.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Appendix B. Prior Coverage

During the past 5 years, the Inspector General, DoD, issued two reports related to DJMS information system security controls. The reports are listed below.

Inspector General, DoD

Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System Reserve Component," August 15, 1997

Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996

This audit followed up on specific recommendations made in those two reports. The prior audits identified problems similar to those discussed in the Finding section of this report, which are identified as repeat findings. The results of the followup made in this audit are summarized in the Table below and are detailed in the report discussion.

Followup Status of Prior Audit Recommendations		
Inspector General, DoD, Report and Recommendation	Corrective Action Taken	Audit Followup Results
Report No. 96-175, Recommendation A.1.a. The Director for Military Pay—Air Force, DFAS Military and Civilian Services (formerly the Director, Directorate of Military Pay, DFAS Denver Center) should direct ISSOs to review and verify user access to master pay datasets, sensitive profiles, multiple user tables, and high-risk owned transactions.	DFAS concurred, stating that corrective action was complete. Regular audits of the master pay datasets, profiles, critical commands (OTRANs) had been made and would continue.	A repeat finding is reported in this report, as discussed under User Access Controls. The prior recommendation was appropriate (and is reiterated in this report). However, current DJMS Security Administrators lacked the technical expertise and training to effectively implement the recommended corrective actions.

Inspector General, DoD, Report and Recommendation	Corrective Action Taken	Audit Followup Results
Report No. 96-175, Recommendation A.1.b. The Director for Military Pay—Air Force should direct ISSOs to review and verify user access to ensure adequate separations of conflicting duties.	DFAS concurred, stating that corrective action was complete. Central site profiles were reviewed and discrepancies corrected to ensure separation of conflicting duties. The "Access" profile was reviewed and critical production datasets were changed to read-only access.	A repeat finding is reported in this report, as discussed under User Access Controls. The prior recommendation was appropriate (and is reiterated in this report). However, current DJMS Security Administrators lacked the technical expertise and training to effectively implement the recommended corrective actions.
Report No. 96-175, Recommendation A.1.c. The Director for Military Pay—Air Force should direct ISSOs to remove Global Access Permission from all sensitive profiles.	DFAS concurred and removed the Global Access Permission attribute from the five profiles.	Audit followup verified that the attribute was removed from sensitive profiles.
Report No. 96-175, Recommendation C.3.a. The Director for Military Pay—Air Force should realign the directorate so that the ISSO reports to the director.	This recommendation was superceded by two recommendations made in Inspector General, DoD, Report No. 99-107 to revise a DFAS information security regulation to define the operational elements of each automated information system over	A repeat finding is reported in this report, as discussed under ISSO independence. The prior recommendation was appropriate but the changes made to the DFAS regulation did not clearly establish an independent chain of command through which ISSOs should report.

Inspector General, DoD, Report and Recommendation	Corrective Action Taken	Audit Followup Results
Report No. 96-175, Recommendation C.3.a. (cont'd)	which ISSOs must enforce security requirements (Recommendation 1.b.(2)), and create a security structure within DFAS that defines the chain of command for ISSOs to ensure they do not report to the identified operational elements (Recommendation 1.b.(3)). In additional comments on that report, DFAS concurred. DFAS revised the regulation to define the operational elements but did not fully implement the second recommendation.	This report reiterates Recommendation 1.b.(3) in Inspector General, DoD, Report No. 99-107.
Report No. 96-175, Recommendation C.3.b. The Director for Military Pay—Air Force should assume responsibility for designating position sensitivity for all positions created within the directorate.	DFAS concurred, stating the sensitivity rating for the three DJMS Air Force-unique ISSOs was upgraded to critical-sensitive.	The condition identified by the prior audit was subsequently incorporated in a DFAS-wide finding and recommendation. See the discussion below for details on the repeat finding reported in this report related to followup made on Report No. 97-203, Recommendation B.3.a.
Report No. 96-175,		

Inspector General, DoD, Report and Recommendation	Corrective Action Taken	Audit Followup Results
Recommendation C.3.c. The Director for Military Pay—Air Force should verify the accuracy of sensitivity levels assigned to all directorate positions.	DFAS concurred, stating that the Defense Security Service was processing required security clearances for directorate positions.	The condition identified by the prior audit was subsequently incorporated in a DFAS-wide finding and recommendation. See the discussion below for details on the repeat finding reported in this report related to followup made on Report No. 97-203, Recommendation B.3.b.
Report No. 97-203, Recommendation B.2. The Director, Directorate for Support Services, DFAS Support Services Denver (formerly Director, Directorate for Software Engineering-Military Pay, DFAS Financial Systems Organization) should request access to DJMS resources directly from DJMS ISSOs.	DFAS concurred, stating that procedures were established to request system access through the DJMS coordinating ISSO.	Audit followup verified that the procedures were developed.
Report 97-203, Recommendation B.3.a. The DFAS Director should emphasize security by requiring each site director (formerly center directors) and the Director for Information and	DFAS partially concurred. Under the mediation agreement with the Inspector General, DoD, the DFAS Director was to issue directions to each site director and the Director	Audit followup was limited to DFAS Denver. A repeat finding is reported in this report, as discussed under Critical-Sensitive Ratings. The prior recommendation was appropriate for a
Report 97-203, Recommendation B.3.a.	for Information and	

Inspector General, DoD, Report and Recommendation	Corrective Action Taken	Audit Followup Results
(cont'd) Technology (formerly Deputy Director, Information Management) to provide written assurance that sensitivity levels are assigned to all personnel positions in accordance with DoD Regulation 5200.2-R.	Technology to verify compliance with personnel security requirements, including the sensitivity assigned to all DFAS positions. These directors would be required to provide the DFAS Director with written assurance when compliance was achieved.	one-time action at the Director's level. However, the recommendation is reiterated in this followup report but specific only to DJMS users. Secondary internal controls were circumvented or not followed. The primary control (the DJMS Security Administrators) failed because most of these security administrators were not adequately trained in their responsibilities in granting system access requests. This report recommends ISSO training and alerts to Denver site managers to the importance of establishing appropriate position descriptions before filling personnel vacancies.
Report No. 97-203, Recommendation B.3.b. The DFAS Director should emphasize security by requiring each site director and the Director for Information and Technology to provide written assurance that all personnel with sensitive access to automated	DFAS partially concurred. In response to the mediation agreement with the Inspector General, DoD, the DFAS Director was to issue directions to each site director and the Director for Information and Technology to verify compliance with personnel	Audit followup was limited to DFAS Denver. A repeat finding is reported in this report, as discussed under Critical-Sensitive Ratings. The prior recommendation was appropriate for a one-time action at the Director's level. However, the recommendation is
Report No. 97-203, Recommendation B.3.b.	security requirements,	reiterated in this followup

Inspector General, DoD, Report and Recommendation	Corrective Action Taken	Audit Followup Results
(cont'd) information systems have background investigations (and where appropriate, interim waivers pending completion of such investigations), as required by DoD Regulation 5200.2-R.	including background investigative requirements for all DFAS positions. These directors would be required to provide the DFAS Director with written assurance when compliance was achieved.	report but specific only to DJMS users. The primary control (the DJMS Security Administrators) failed because most of these security administrators were not adequately trained in their responsibilities in granting system access requests. This report recommends ISSO training.

Appendix C. File Transfer Protocol

The DJMS System Manager identified security risks in the use of a locally developed, file transfer protocol, which was called the File Transfer Interface. This file transfer protocol was used by the DJMS application to transfer data between locations. Although not part of our audit objectives, we evaluated the corrective action taken by management related to this file transfer protocol.

The DJMS System Manager determined that the File Transfer Interface software did not adequately control the DJMS data that it sent and received from remote locations. Specifically, user IDs for the File Transfer Interface were shared, the passwords were non-expiring, and the identity of the transfer source was not validated. The File Transfer Interface software completed a series of systemic, high-level qualifier validations to either accept or reject data in a DJMS update. However, these validations did not mitigate the risks developed by sharing user IDs or using non-expiring passwords. As a result, DJMS data could be compromised.

We determined that the Departmental Accounting Systems Support Branch, Directorate for Technology Services, DFAS Support Services Denver, was actively working with DISA Mechanicsburg to find a suitable file transfer software that meet the security requirements of both DFAS and DISA. In addition, unique user IDs will be required to use the File Transfer Interface.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
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

Non-Defense Federal Organizations

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Defense Finance and Accounting Service Comments

Final Report Reference

DEFENSE FINANCE AND ACCOUNTING SERVICE
KANSAS CITY, MISSOURI 64197-0001

DFAS-PSM/DE

MAY 2 2 2001

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, ARLINGTON, VIRGINIA

SUBJECT: Comments on Draft Audit Report on Defense Joint Military Pay System Security Functions at Defense Finance and Accounting Service Denver (Project No. D2000FG0052.001), dated March 16, 2001

The requested comments to the subject draft audit report are provided below:

Recommendation 1.a.(1): "The Director, Defense Finance and Accounting Service, revise the Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management (IM) Corporate Policy," Part G., Chapter 1, "DFAS Information Assurance Policy," July 18, 2000, to specify that information system security officers (ISSOs) shall report directly to the project or system manager for each information system, where appropriate or to functional application managers at each agency site such as the Director for Military Pay - Air Force."

See revised recommendation and Finding discussion of ISSO independence.

DFAS Comments: Non-Concur.

Rationale for Non-concurrence: The same ISSO reporting issue described in this report has been successfully mediated in the response to the audit report for the Defense Civilian Pay System, dated August 13, 2000. As a result of the mediation agreement, dated December 21, 1999, DFAS has revised DFAS Regulation 80001.1-R to provide autonomy for ISSOs when enforcing requirements over operational elements. ISSMs appoint in writing an ISSO for each information system that receives its primary support within the ISSM's activity. To further promote ISSO independence, an ISSO cannot be assigned to the end-user population of the system or to a Central Design Activity directly supporting a production system. ISSOs report security incidents, vulnerabilities and assessments to the supporting ISSM with an advisory to the PM/SM. DFAS implemented the new procedures in July 2000 and feels that time is needed to prove its effectiveness.

Audit report date was March 16, 1999, not August 13, 2000.

Recommendation 1.a.(2): "We recommend that the Director, Defense Finance and Accounting Service, revise the Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management (IM) Corporate Policy," part G., Chapter 1, "DFAS Information Assurance Policy," July 18, 2000, to: Specifically identify and establish a minimum level 2 training requirement for information system security officers in the discussion of training requirements in paragraph 7.9."

DFAS Comments: Concur. DFAS will re-evaluate its Information Assurance (IA) Training and Certification Plan to ensure that IA personnel are trained to perform the tasks associated with their designated responsibilities for safeguarding DFAS information systems. DFAS will identify and establish training requirements for IA personnel (i.e., ISSMs, ISSOs, and TASOs) at a level equivalent to Level 2 for system administrators. ECD: December 31, 2001.

Recommendation 1.b: "We recommend that the Director, Defense Finance and Accounting Service, revise Memorandum of Agreement on the Defense Joint Military Pay System, June 15, 2000, in concert with the changes recommended to Defense Finance and Accounting Service Regulation 8000.1-R."

DFAS Comments: Concur. The Memorandum of Agreement on the Defense Joint Military Pay System, June 15, 2000, will be updated to reflect the Defense Finance and Accounting Service Regulation 8000.1-R. changes identified in recommendation 1.a(2). ECD: January 31, 2002.

Recommendation 2.a.(1): "The Director for Defense Joint Military Pay System Centralized Systems Management, Defense Finance and Accounting Service Denver, direct the information systems security officer to review all user permissions and verify that proper separation of conflicting duties is maintained among users and sensitive access to datasets, profiles, owned transactions, and other Defense Joint Military Pay System core resources is granted in accordance with DoD Regulation 5200.2-R, "Personnel Security Program," January 1987."

DFAS Comments: Concur. User permissions are continuously being reviewed on the DJMS. Separation of duties is maintained among users by checking for conflicting profiles on userids and conflicting access levels on CICS regions within profiles. Critical datasets with more than "read" access have been identified and an audit attribute has been added to them. Owned transactions (OTRANs) that have been identified as sensitive have been audited and/or placed in profiles and checked for separation of duties. File Transfer Protocol (FTP) userids are restricted to only authorized users and are audited. Userids are checked for last used dates and suspended or deleted based on that date, as applicable. ECD: Completed September 30, 2000.

Recommendation 2.a.(2): "The Director for Defense Joint Military Pay System Centralized Systems Management, Defense Finance and Accounting Service Denver, direct the information systems security officer to annually provide and report upon training given to supervisors and security administrators on their responsibilities in preparing and processing the Defense Information Systems Agency (DISA) Form 41, "System Authorization Access Request." Annual attendance at such training should be mandatory for all supervisors who request user access to system core resources and for security administrators over the system's core and Air Force-unique resources."

DFAS Comments: Concur. The DJMS Core Security Office has prepared and presented DJMS specific training to all core supervisors and TASOs. The annual training provides specific instruction relating to DJMS to include DISA Form 41, "System Authorization Access Request" preparation and processing, password review, and Computer Associates Top Secret (CA-TSS) security software "list" and "reset" command instructions. The attendance of this training was documented and will be maintained by the DJMS Core Security Office. ECD: Completed January 30, 2001.

Recommendation 2.a.(3): "The Director for Defense Joint Military Pay System Centralized Systems Management, Defense Finance and Accounting Service Denver, direct the information systems security officer to validate and document all user access to the corresponding DISA Form 41, 'System Authorization Access Request'."

DFAS Comments: Concur. The DJMS Core Security Office has reviewed and validated all core users DISA Form 41s. Additionally, supporting documentation has been attached to the DISA Form 41s to provide further audit trail, clarification, and justification. ECD: Completed September 14, 2000.

Recommendation 2.a.(4): "The Director for Defense Joint Military Pay System Centralized Systems Management, Defense Finance and Accounting Service Denver, direct the information systems security officer to annually require that supervisors over system users provide written assurance that position descriptions for system users are assigned the proper sensitivity level and that system users (including contractors) with critical-sensitive access to automated information systems have background investigations (and where appropriate, interim waivers pending completion of such investigation), as required by DoD 5200.2-R."

DFAS Comments: Concur. Supervisors are required to annually certify an Assurance Statement certifying all position descriptions for system users are assigned the appropriate sensitivity level to include that their employees with critical-sensitive access have the appropriate level of background investigation. The DJMS Core Security Office maintains the Assurance Statements. Additionally, before a user is permitted a hi level of critical access, the user must provide a correctly prepared DISA Form 41 to include proof of the appropriate background investigation and/or a valid security waiver, as applicable. ECD: May 31, 2001.

Recommendation 2.b: "The Director for Defense Joint Military Pay System Centralized Systems Management, Defense Finance and Accounting Service Denver, verify that position descriptions with correct sensitivity ratings are approved for each position before filling current and future vacancies on the system's core security team."

DFAS Comments: Concur. Position descriptions with the correct sensitivity rating for each position in the DJMS Core Security Office are approved. Additionally, prior to filling future vacancies, position descriptions will be reviewed to ensure that the appropriate sensitivity ratings are represented. ECD: Completed September 8, 2000.

Recommendation 3.a: "The Director, Directorate for Military Pay - Air Force, Defense Finance and Accounting Service Denver, direct the ISSOs to review all user permissions and verify that proper separation of conflicting duties is maintained among users and sensitive access to datasets, profiles, owned transactions, and other Defense Joint Military Pay System Air Force-unique resources is granted in accordance with DoD Regulation 5200.2-R."

DFAS Comments: Concur. The DISA Forms 41 and the individual's records have been reviewed to ensure that conflicting profiles are not assigned. Additionally, Air Force Military Pay Operations is developing written procedures for modifying conflicting profiles. ECD: May 31, 2001.

Recommendation 3.b: "The Director, Directorate for Military Pay - Air Force, Defense Finance and Accounting Service Denver, direct the ISSOs to attend the annual training required by Recommendation 2.a. (2) and annually provide and report upon training given to supervisors on their responsibilities in preparing and processing the DISA Form 41, 'System Authorization Access Request'. Annual attendance at such training should be mandatory for all supervisors who request user access to Air Force-unique system resources."

DFAS Comments: Non-concur.

Rationale for Non-concurrence: DFAS-TDMS/DE, Information System Security, provides annual training on various aspects of information security for the Denver users. Each location has similar requirements for security training. DFAS-DEM 7073-1, Chapter 3, provides instructions on the DISA Form 41; a revision to the chapter was disseminated in April 2001. In addition, the Denver ISSOs have a dedicated electronic mailbox if anyone has additional questions. A training course, designed for the various locations serviced by the Denver ISSOs, would be cumbersome and redundant.

Recommendation 3.c: "The Director, Directorate for Military Pay - Air Force, Defense Finance and Accounting Service Denver, direct the ISSOs to validate and document all user access to the corresponding DISA Form 41, 'System Authorization Access Request.'"

DFAS Comments: Concur. DISA Forms 41 are reviewed when they are submitted. In addition, other routine reports document irregularities or non-use and appropriate action is taken. ECD: Completed October 27, 2000.

Recommendation 3.d: "The Director, Directorate for Military Pay - Air Force, Defense Finance and Accounting Service Denver, direct the ISSOs to annually require that supervisors of the system users provide written assurance that position descriptions for system users (including contractors) are assigned the proper sensitivity level and that access to automated information systems have background investigations (and where appropriate, interim waivers pending completions of such investigations), as required by DoD 5200.2-R."

DFAS Comments: Non-concur.

Rationale for Non-Concurrence: The position descriptions for the ISSOs assigned to DFAS-PMJ/DE are properly coded as critical sensitive. As an essential part of the hiring process, the immediate supervisors are responsible for reviewing position descriptions to determine their needs. Human Resources is responsible for reviewing the position descriptions for general compliance items and reviewing the qualifications of the individuals presented to management for consideration.

Recommendation 4: The Director, Human Resources Defense Finance and Accounting Service Support Services, Denver, establish procedures to periodically alert site supervisors to the importance of and requirement that appropriate position descriptions be established for all personnel positions before filling such vacancies by promotion or reassignment."

DFAS Comments: Concur. The Denver Human Resources Customer Support Unit sent a memo to all directors on January 16, 2001 advising that appropriate position descriptions must be established for all positions before filling vacancies. In addition, this memo also advised that when an employee is placed in another position, even on a temporary basis, the employee must meet the position sensitivity and any physical requirements of the new position. This periodical alert will be done on an annual basis at the beginning of the calendar year.
ECD: Completed January 16, 2001.

Questions your staff may have concerning these matters may be directed to my point of contact, Ms. Sue Schallenberg, DFAS-PSM/DE, (303) 676-7541.

Steve E. Turner
Director, Military and Civilian Pay Services

cc:
DFAS-DDI/AR

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Paul J. Granetto
Richard B. Bird
Brian M. Flynn
W. Andy Cooley
Thomas G. Hare
Mary K. Reynolds
Stephen G. Wynne
Lisa C. Rose-Pressley