

Audit



Report

SELECTED GENERAL CONTROLS OVER THE RETIREE AND
CASUALTY PAY SUBSYSTEM AT THE DEFENSE FINANCE
AND ACCOUNTING SERVICE CLEVELAND CENTER

Report Number 98-098

March 30, 1998

Office of the Inspector General
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 or visit the Inspector General, DoD, Home Page at: WWW.DODIG.OSD.MIL.

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) 604-8908 (DSN 664-8908) 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 to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DRAS	Defense Retiree and Annuitant Pay System
OMB	Office of Management and Budget



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

March 30, 1998

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE

SUBJECT: Audit Report on Selected General Controls Over the Retiree and Casualty Pay Subsystem at the Defense Finance and Accounting Service - Cleveland Center (Report No. 98-098)

We are providing this audit report for information and use. The audit was conducted in support of our financial statement audits required by the Chief Financial Officers Act of 1990 and the Federal Financial Management Act of 1994. This report is the first in a series of reports that will be issued on the Defense Retiree and Annuitant Pay System.

We considered management comments on a draft of this report in preparing the final report. The Defense Finance and Accounting Service comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Kimberley Caprio, Audit Program Director, at (703) 604-9139 (DSN 664-9139) or Mr. Dennis L. Conway, Audit Project Manager, at (703) 604-9158 (DSN 664-9158). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-098
(Project No. 6FG-0093)

March 30, 1998

Selected General Controls Over the Retiree and Casualty Pay Subsystem at the Defense Finance and Accounting Service Cleveland Center

Executive Summary

Introduction. The audit was conducted to support our audits required by the Chief Financial Officers Act of 1990 and the Federal Financial Management Act of 1994. This report is the first in a series of reports resulting from our audit of the Defense Retiree and Annuitant Pay System. The report addresses our review of the general controls over the Defense Finance and Accounting Service Cleveland Center Retiree and Casualty Pay Subsystem (the Subsystem)--one of the two subsystems in the Defense Retiree and Annuitant Pay System.

The Subsystem was used to account for 1.8 million retirees and to disburse an average of \$2.3 billion each month from the DoD Military Retirement Trust Fund in FY 1997. The high volume and dollar value of transactions processed makes effective controls over the Retiree and Casualty Pay Subsystem essential to ensuring the production of authorized, accurate, complete, and reliable retired pay data for the Fund.

Audit Objectives. The overall objective was to evaluate general and application controls over the Defense Retiree and Annuitant Pay System to ensure the production of authorized, accurate, complete, and reliable data. This report addresses our review of the general controls over the Retiree and Casualty Pay Subsystem. (General controls are management controls that apply to the overall computer operations of an organization). Also, we reviewed the management control program as it related to the Retiree and Casualty Pay Subsystem.

Audit Results. The Defense Finance and Accounting Service had implemented controls to include establishing an overall security program, implementing procedures for developing and changing computer software (such as computer programs), separating duties that could allow undetected and unauthorized or fraudulent activity to occur, establishing controls to monitor the use of a system's software, and establishing procedures for preventing disruptions in service to customers. Additional controls were needed for monitoring and updating the security program, limiting access to the Subsystem, and providing for continuity of operations.

Although we did not detect unauthorized or fraudulent activity, the need for improved controls over the Subsystem increases the possibility of such activity occurring. Implementation of these controls would increase the level of confidence that managers can place on the authorization, the accuracy, the completeness, and the reliability of retired payments.

Additional management controls recommended in this report will:

- o reduce the possibility that fraudulent activity occurs or ensure it can be detected in a timely manner, and

- o ensure the continuity of operations in case of a disaster. See Appendix A for details on the management control program and Part I for a discussion of the audit results.

Summary of Recommendations. We recommend that the Director, Defense Finance and Accounting Service Cleveland Center, update security documents, monitor access to the Subsystem, and establish improved controls over the security of the Subsystem.

Management Comments. The Deputy Director for Finance, Defense Finance and Accounting Service Cleveland Center, agreed to update security documents, monitor daily reports of accesses to the Subsystem, and conduct periodic reviews to identify deficiencies in the security controls over the Subsystem. The Defense Finance and Accounting Service Cleveland Center requested clarification of information regarding security clearance levels assigned by Center personnel for security officer positions. The Center was concerned that the draft report inferred security clearance levels were not designated for security officer positions.

The Center also requested the basis for the assistant information security officer position to be designated critical sensitive, the same level of clearance as the information security officer position. See Part I for a complete discussion of the management comments and Part III for the complete text of the management comments.

Audit Response. Our intent with regards to security clearance levels was not to infer that clearance levels were not designated, but, to request that management review the appropriateness of existing clearance levels. Further, in the information security officer's absence, the assistant officer would perform the information security officer's duties, therefore, we contend that the assistant officer should possess an equivalent level of clearance. Defense Finance and Accounting Service comments were responsive to the recommendations; therefore, no further comments are required.

Table of Contents

Executive Summary	i
Part I - Audit Results	
Audit Background	2
Audit Objectives	2
Controls Over the Retiree and Casualty Pay Subsystem	4
Part II - Additional Information	
Appendix A. Audit Process	
Scope and Methodology	16
Management Control Program	17
Appendix B. Summary of Prior Coverage	19
Appendix C. Major Categories of General Controls	22
Appendix D. Report Distribution	23
Part III - Management Comments	
Defense Finance and Accounting Service Comments	26

Part I - Audit Results

Audit Background

This report is the first in a series resulting from our ongoing audit of the Defense Retiree and Annuitant Pay System. The audit was conducted to support our audits required by the Chief Financial Officers Act of 1990 and the Federal Financial Management Act of 1994.

On August 8, 1991, the DoD Corporate Information Management Financial Management Steering Committee approved the Defense Finance and Accounting Service (DFAS) proposal to standardize and consolidate DoD retiree and annuitant pay systems.

The DFAS Cleveland Center Retired Pay System and the DFAS Denver Center Annuitant Pay System were chosen to be integrated as the Defense Retiree and Annuitant Pay System (DRAS). The Cleveland Center Retired Pay System was renamed the Retiree and Casualty Pay Subsystem and the Denver Center Annuitant Pay System was renamed the Annuitant Pay Subsystem.

Retiree and annuitant pay transactions are processed on computers managed by the Defense Information Systems Agency (DISA). The DISA Defense Megacenters located at Chambersburg, Pennsylvania, processes transactions for the DFAS Cleveland Center Retiree and Casualty Pay Subsystem. The Defense Megacenters located at Denver, Colorado, processes transactions for the DFAS Denver Center Annuitant Pay Subsystem.

This report discusses our review on selected general controls over the DFAS Cleveland Center Retiree and Casualty Pay Subsystem. The Subsystem was used to account for 1.8 million retirees and to disburse a monthly average of \$2.3 billion from the DoD Military Retirement Trust Fund in FY 1997.

Audit Objectives

The overall audit objective was to evaluate general and application controls over the Defense Retiree and Annuitant Pay System to ensure the production of authorized, accurate, complete, and reliable data. The report addresses our review of the general controls over the Retiree and Casualty Pay Subsystem. Also, we reviewed the management control program as it related to the Retiree and Casualty Pay Subsystem.

See Appendix A for a discussion of the audit scope, methodology, and the management control program, and Appendix B for a summary of prior coverage related to the audit objectives.

Controls Over the Retiree and Casualty Pay Subsystem

The DFAS Cleveland Center needed to improve critical information system security controls over the Retiree and Casualty Pay Subsystem. Three categories of security controls needing improvement were monitoring and updating the security program, controls over access to the subsystem, and providing for continuity of operations.

Information system security controls were not fully implemented or maintained because the DFAS Cleveland Center had not ensured compliance with some security requirements. The absence of these security controls increases the possibility for unauthorized or fraudulent activity to occur or to not be detected in a timely manner. Also, the absence of these controls lowers the confidence that managers can place on the authorization, the accuracy, the completeness, and the reliability of retired payments.

System of Internal Controls

Office of Management and Budget (OMB) Circular No. A-127, "Financial Management Systems," July 23, 1993, states that financial management systems shall include a system of internal controls that ensures resource use is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data are obtained, maintained, and disclosed in reports. These system-related controls form a portion of the management control structure required by OMB Circular No. A-123, "Management Accountability and Control," June 21, 1995.

Also, OMB Circular No. A-127 states that agencies shall plan for and include security controls in financial management systems in accordance with OMB Circular No. A-130, "Management of Federal Information Resources," February 8, 1996. OMB Circular No. A-130 establishes a minimum set of controls to be included in automated information system security programs.

DoD information systems should include a minimum of six major categories of general controls. General controls are management controls that apply to the overall computer operations of an agency or an organization and include the following:

- o establishing an overall security program,
- o limiting access to automated systems,
- o implementing procedures for developing and changing computer software (for example, changing computer programs),
- o separating duties that could allow undetected and unauthorized or fraudulent activity to occur,
- o establishing controls to monitor the use of a system's software, and
- o establishing procedures for preventing disruptions in service to customers.

See Appendix C for a definition of the major categories of general controls.

Information System Controls

Three categories of security controls needed improvement--monitoring and updating the security program, controls over access to the subsystem, and providing for continuity of operations.

Monitoring and Updating Security-Related Changes. The DFAS Cleveland Center was not fully monitoring and updating security-related changes in its security program. Specifically, the risk assessment and the security plan were not updated when facilities, operations, and risks changed; security personnel did not have appropriate training, experience, or levels of security clearance; and the Retiree and Casualty Pay Subsystem was not accredited as required.

Development of a Risk Assessment. OMB Circular No. A-130 requires the development of a risk assessment that includes the value of a system, analysis of threats and vulnerabilities, and the effect of current or proposed safeguards.

The DFAS Cleveland Center had developed a risk assessment as of June 9, 1994; however, significant changes had occurred for processing retired payments. For example,

- o Marine Corps and Army retired pay accounts were relocated to and processed by the Cleveland Center as of July 1994 and April 1995, respectively (these two Military Services were responsible for 722,000 retired pay accounts as of March 20, 1997), and

- o retired pay accounts processed at Bratenahl, Ohio, (a suburb of Cleveland, Ohio) were relocated to Chambersburg, Pennsylvania.

Controls Over the Retiree and Casualty Pay Subsystem

By updating and assessing changes affecting the Subsystem, the DFAS Cleveland Center could lessen potential risks to its data.

Security Plans for Retired Pay Operations. The security plans for retired pay operations were not updated to include new facilities, operations, and risks. DFAS Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," August 23, 1996, states that the information security officer is responsible for ensuring that security plans are developed and maintained.

The DFAS Cleveland Center had developed two security plans. One plan, dated July 9, 1993, provided guidance for securing the DRAS operations. The other plan, dated July 1994, provided guidance for securing computer operations at the three buildings that housed DFAS Cleveland Center personnel and computer equipment.

Neither security plan had been updated to reflect current operating conditions. For example, the plan for DRAS operations stated that it provided security guidance for a computer in Cleveland, Ohio. However, computer processing of retired pay by DRAS was transferred on August 27, 1995, to the Defense Megacenter at Chambersburg, Pennsylvania. The other plan stated that when computer terminals were unattended, adequate security was provided by locked doors. However, computer terminals were located in offices without locked doors.

The process of updating the security plans to reflect current facilities, operations, and risks of the Retiree and Casualty Pay Subsystem could identify deficiencies for corrective action that would improve security over the Subsystem's data.

Security-Related Training and Experience. The DFAS Cleveland Center did not fully ensure that personnel had the necessary security-related training and experience. The National Computer Security Center's "A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems," May 1992, states that an information system security officer should have the following minimum qualifications to provide a solid technical background:

- o two years of experience in a computer-related field,
- o one year experience in computer security, or mandatory attendance at a computer security training course,
- o familiarization with the operating system of the AIS (Automated Information System), and
- o a technical degree is desirable in computer science, mathematics, electrical engineering, or a related field.

Controls Over the Retiree and Casualty Pay Subsystem

Of the 11 information system security officers with retired pay responsibilities, only 6 met at least 1 of the minimum requirements. The DFAS Cleveland Center could identify better qualified information system security officers by evaluating the security-related training and experience of its candidates.

Levels of Security Clearances. The levels of security clearances were not reviewed before DFAS personnel were assigned to security duties. DoD Regulation 5200.2-R requires each civilian position in DoD to be classified as critical-sensitive, noncritical-sensitive, or nonsensitive.*

The DFAS Cleveland Center had appropriately identified the information security officer as occupying a critical-sensitive position and had conducted an investigation into the background of the security officer. (An extensive background investigation is normally conducted before assignment to critical-sensitive jobs). However, the assistant information security officer's position was classified as noncritical-sensitive; a less extensive National Agency Check with written inquiries was completed.

The classification of noncritical-sensitive would be appropriately assigned to information system security officers (information system security officers are subordinate to information security officers). In the absence of the information security officer, the assistant information security officer would assume those duties; therefore, the assistant information security officer's position should also be identified as critical-sensitive and be subject to the more extensive background investigation.

Also, only 2 of the 11 information system security officers assigned to the Retired Pay Directorate were occupying positions classified as noncritical-sensitive. The positions for the other nine information system security officers were classified as nonsensitive. (All information system security officer positions should be classified as noncritical-sensitive because these officers have access to personal information.) Further, neither the information security officer nor the Security Directorate were aware of the sensitivity levels for these information system security officers.

By having the sensitivity levels reviewed by qualified security personnel (that is, personnel who have knowledge of the level of security responsibilities) and by requiring the appropriate background investigations before assigning personnel to security officer duties, the DFAS Cleveland Center would reduce its risk for assigning inappropriate personnel to security duties.

Accreditation of DRAS. DFAS Cleveland Center managers had not conducted an accreditation of DRAS when significant changes had occurred.

*Critical-sensitive positions for information systems personnel include responsibilities for planning, directing, and implementing a computer security program. Noncritical-sensitive positions include responsibilities for monitoring systems that allow access to or processing of personal data. Also, personnel assigned to noncritical-sensitive positions perform work that is reviewed by personnel occupying critical-sensitive positions. All other positions are classified as nonsensitive positions.

Controls Over the Retiree and Casualty Pay Subsystem

OMB Circular No. A-130 requires managers to authorize the use of a system before beginning or significantly changing processing in it. After a system has been authorized (accredited) for use, it should be reaccredited every 3 years.

In addition, the National Computer Security Center's "Introduction to Certification and Accreditation," January 1994, states that management must continually track and reassess the level of security in a system. Based on these reassessments, management must decide whether the level of security is sufficient to allow the system to continue to operate.

No documentation was provided to show that DFAS Cleveland had accredited the Retiree and Casualty Pay Subsystem. As previously stated, significant changes had occurred that deserved reassessment of the level of security. In addition, the Defense Megacenter that processed retired pay was only accredited to operate on an interim basis.

By analyzing and accrediting the Subsystem, DFAS Cleveland Center management could better ensure that the level of security over the operation of the Retiree and Casualty Pay Subsystem was sufficient. Reaccreditations should be made when significant changes occur.

Controls Over Access to the Retiree and Casualty Pay Subsystem. Controls over access to the Retiree and Casualty Pay Subsystem were not always sufficient to protect the Subsystem and its data from potential misuse or destruction. Information security managers had not always produced or reviewed reports showing access to the Subsystem, and physical access to retired pay areas and computer facilities was sometimes not properly limited.

Frequency of Users' Accesses to the Subsystem. Information security managers could not fully monitor unusual activity because they were not consistently producing and reviewing reports showing the frequency of user access to the Subsystem. DoD Standard 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 26, 1985, states that controls must be in place to protect automated systems from unauthorized access. These controls should ensure that security procedures are in place to create, maintain, and protect an audit trail of access to a system's programs and files.

For the Retiree and Casualty Pay Subsystem, the Access Control Facility 2 software--produced by Computer Associates International, Incorporated--provides this protection. The Access Control Facility 2 software can produce daily reports that provide an audit trail of access to a system.

Despite the availability of these reports, DFAS Cleveland Center security personnel were not always producing or using the reports. Therefore, security personnel lacked an audit trail for detecting unusual or potentially illegal access to the Subsystem's files.

The DFAS Cleveland Center had developed DFAS-CL 5215.1-G, "A User's Guide to Computer Security," July 1994, to provide guidance for monitoring

Controls Over the Retiree and Casualty Pay Subsystem

user access to the Subsystem. The guide states that the Information Security Office will review to ensure that new users actually use their privilege to access a system. If new users have not accessed a system within a 2-week period, the access privilege will be deleted. The guide also states that the Information Security Office will delete the access privileges of any user that has not accessed a system for a period of 90 days.

Special reports produced by the Access Control Facility 2 software showed how frequently users had accessed a system. As of November 15, 1996, 90 of 107 new users (84.1 percent) had not accessed the system in more than 60 days. In addition, no access was reported for 21 of the 107 new users (19.6 percent) since December 1995. The Information Security Office had not removed these new users' access privileges.

For other than new users, no access was reported for 246 of 288 users (85.4 percent) in over 120 days. In addition, no access was reported for 83 of the 246 users (33.7 percent) since at least calendar year 1995. For three users, no access was reported since calendar year 1994. At the time of this review, the Information Security Office had not removed any of these users' access privileges. The absence of monitoring infrequent access to the system decreases the opportunity for identifying and eliminating, in a timely manner, users that have not demonstrated a need for accessing the retired pay subsystem.

Further, the DFAS Cleveland Center had not established controls to monitor access to the system by some information system security officers. The DFAS Cleveland Center had two information system security officers that could independently establish a user's account and authorize that user access to specific files in the subsystem. (A user's account includes information such as the user's name, Social Security number, and position title). Therefore, these information system security officers could grant themselves or other users access to specific files in the Subsystem although that access was not needed or authorized by management to perform retired pay duties. The Information Security Office had not produced any reports from the Access Control Facility 2 software to monitor unusual accesses granted by the information system security officers.

More control over identifying unusual or potentially illegal access to the subsystem could be achieved by the Information Security Office monitoring accesses to the system and investigating unusual use of the system.

Access to DFAS Offices and the Retiree and Casualty Pay Subsystem. Access to DFAS offices and the Retiree and Casualty Pay Subsystem was not always properly limited. DoD Directive 5200.28-STD, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, states that information systems shall be protected to prevent unauthorized disclosure, destruction, and modification.

The DFAS Cleveland Center had employees with computer access to the Retiree and Casualty Pay Subsystem in the North Point Towers Building and in the Anthony J. Celebreeze Federal Building (the Federal building) in Cleveland, Ohio. DFAS shares working space in both buildings with other Federal

Controls Over the Retiree and Casualty Pay Subsystem

organizations; therefore, security was needed in both locations to protect the Retiree and Casualty Pay Subsystem.

Unauthorized personnel could not obtain access to the retired pay offices in the North Point Towers Building without either an access code to the automated security system or an escort. However, improvements were needed in the security at the Federal building. The guards in the Federal building checked for identification badges, but they still allowed employees without badges and visitors unescorted access to the building. The DFAS Cleveland Center had recognized the need for better security at the Federal building and had obtained badges for use by visitors. However, the badges were not used.

The Federal building housed DFAS computers that had access to the Retiree and Casualty Pay Subsystem. These DFAS computers were located in unlocked offices, and anyone allowed access into the Federal building could enter these offices. Although DFAS computers in the Federal building were not available for use by the public, a malicious act by a single unauthorized individual to defraud or destroy retired pay data could result in disastrous consequences to the integrity of the Retiree and Casualty Pay Subsystem.

Access to DFAS offices and its computers in the Federal building could be restricted by establishing and enforcing better security measures such as issuing badges to visitors and locking doors to DFAS office areas.

Supporting Critical Operations. Resources and facilities were not identified for supporting critical operations in the event of a disaster. DoD Directive 3020.26, "Continuity of Operations (COOP) Policy and Planning," May 26, 1995, states that DoD Components shall designate alternate headquarters or emergency relocation sites.

The DFAS Cleveland Center developed a contingency plan in October 1994 that addressed obtaining office space, equipment, and supplies in Cleveland, Ohio, if the current office space and equipment were rendered not useable by some event, such as a disaster. The DFAS Cleveland Center had not developed a plan for moving retired pay operations (such as personnel and equipment) to an alternate site geographically separated from Cleveland, Ohio, if a disaster occurs that affects the entire Cleveland, Ohio, metropolitan area. Unnecessary interruptions in the payment of more than 1.8 million retiree pay accounts could be avoided by identifying office space and equipment to support critical operations in the event of a disaster.

Compliance with Security Requirements

Information system security controls were not fully implemented or maintained because the DFAS Cleveland Center had not ensured compliance with some security requirements for the Retiree and Casualty Pay Subsystem. DFAS Regulation 8000.1-R, "Information Management Policy and Instructional

Controls Over the Retiree and Casualty Pay Subsystem

Guidance," August 23, 1996, states that the Directors of each DFAS Center, the Centers' information security officers, and the information system security staff have the first-line responsibility for ensuring compliance with information system security requirements.

The information security officer at a DFAS Center is the key individual responsible for ensuring that security controls are implemented. The information security officer is responsible, in part, for ensuring that:

- o security policies and safeguards are enforced for all personnel having access to an automated information system,
- o all users have been properly trained and are familiar with security policies and procedures before being granted access to the system,
- o audits are reviewed periodically to identify unauthorized users' actions,
- o protective or corrective measures are implemented if a security problem exists,
- o the security status of the system is reported to the Center's director,
- o known or suspected vulnerabilities are evaluated to determine whether additional safeguards are needed,
- o security plans are developed and maintained,
- o contingency plans are developed and tested at least annually,
- o documentation is developed and maintained to support accreditations of automated information systems, and
- o users are removed from access lists if no need exists for accessing a system.

Furthermore, the Director of each DFAS Center has overall responsibility for ensuring that appropriate security controls are implemented and maintained. The Director, DFAS Cleveland Center, would have greater oversight and assurance that security controls have been implemented and maintained by requiring periodic reviews on the controls over the Retiree and Casualty Pay Subsystem.

Conclusion

The inadequate security controls in the Retiree and Casualty Pay Subsystem increases the possibility for unauthorized or fraudulent activity to occur or to not be detected in a timely manner. Also, the inadequate controls lowers the confidence that managers can place on the authorization, the accuracy, the completeness, and the reliability of retired payments.

Deficiencies were identified in monitoring and updating the security program, controls over access to the subsystem, and providing for continuity of operations. Prior audits on DFAS systems have reported the need for similar improvements as shown in this report. (See Appendix B for a summary of prior audit coverage.)

Although we did not review controls over security in other systems at the DFAS Cleveland Center, the potential exists for weaknesses similar to those described in this report. The Director's implementation of recommendations in this report should improve controls over all of the Center's systems.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Defense Finance and Accounting Service Cleveland Center:

- 1. Update the risk assessment and the security plans to reflect current facilities, operations, and risks. The plan should be updated when significant changes occur in facilities, operations, or risks.**
- 2. Evaluate the training and experience of personnel prior to their selection for security-related responsibilities to ensure that candidates have the minimum security training and experience qualifications.**
- 3. Review sensitivity levels of security personnel positions and require appropriate background investigations before assigning personnel to security positions.**
- 4. Correct any deficiencies that can prevent the accreditation of the retired pay subsystem. Conduct reaccreditations when significant changes occur.**
- 5. Monitor accesses to the system and investigate unusual use of the system.**

Controls Over the Retiree and Casualty Pay Subsystem

6. Limit access to offices and computer equipment in the Federal building.

7. Identify office space and equipment needed to support critical operations at an alternate site in the event of a disaster.

8. Conduct periodic reviews and correct any identified deficiencies in the security controls over the Retiree and Casualty Pay Subsystem.

Management Comments. DFAS Cleveland Center management concurred, stating that actions have been or will be taken by March 31, 1998, to implement the recommendations.

Specifically, DFAS agreed to:

- o update the risk assessment and security plans and review the documents annually or when significant changes occur;

- o select security officers that meet the National Computer Security Center's training and experience requirements;

- o review sensitivity levels of security personnel positions, identify personnel without appropriate background investigations, and initiate investigations for these personnel;

- o complete the reaccreditation program and conduct reaccreditations in the future when significant changes occur;

- o develop procedures for monitoring daily reports of system accesses;

- o limit access to offices and computer equipment in the Federal building;

- o identify office space and equipment needed to support critical operations at an alternate site in the event of a disaster and use the General Services Administration, other DFAS Centers, DFAS operating locations, and other Government agencies as alternate sites depending on the severity of the disaster; and

- o conduct periodic reviews and correct deficiencies identified in the security controls over the Retiree and Casualty Pay Subsystem through procedures such as monitoring daily reports on accesses made to the Subsystem.

DFAS Cleveland Center management also requested clarification of information relating to Recommendation 3. Management was concerned that the draft report inferred security clearance sensitivity levels were not designated for security officer positions.

Also, DFAS Cleveland Center management requested the basis for the assertion that the assistant information security officer position be designated critical

Controls Over the Retiree and Casualty Pay Subsystem

sensitive, the same level of clearance as the information security officer position.

Audit Response. Our intent in Recommendation 3 was not to infer that security clearance sensitivity levels did not exist, rather to request that management review the appropriateness of existing security levels. In the information security officer's absence, the assistant officer would perform the information security officer's duties and therefore should possess an equivalent level of clearance. Thus, we recommended the need to review sensitivity levels and to grant the same level of sensitivity to positions with the same duties. DFAS comments were responsive to the recommendations; therefore, no further comments are required.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

Scope and Methodology of Audit. The scope of the audit included reviews of general controls related to the Retiree and Casualty Pay Subsystem of the DRAS. Specifically, we:

- o reviewed security plans and assessments of risk prepared by DFAS personnel,
- o assessed employees' experience and training qualifications on automated information systems and computer security,
- o evaluated controls for ensuring that accreditations were completed and updated,
- o analyzed reports showing frequency of access attempts into the Retiree and Casualty Pay Subsystem,
- o monitored access to DFAS offices and computer equipment,
- o assessed independence and authority of the information security officer and information system security officers to perform their assigned duties,
- o reviewed plans for continuing operations, and
- o interviewed security, human resource management, and retired pay personnel assigned to the DFAS Cleveland Center.

Also, we reviewed policies and procedures related to establishing and maintaining general controls. This guidance was provided in regulations, directives, circulars, or standards developed by OMB, DoD, and the National Computer Security Center.

The Retiree and Casualty Pay Subsystem was used to process transactions for 1.8 million retirees and to disburse a monthly average of \$2.3 billion from the DoD Military Retirement Trust Fund in FY 1997.

Use of Computer-Processed Data. We used reports generated by security software packages to review the general controls established for the Retiree and Casualty Pay Subsystem. Data were used from the Access Control Facility 2 security software--produced by Computer Associates International, Incorporated--to review the extent of access allowed to key retired pay and security personnel. The Retiree and Casualty Pay Subsystem was used to process sensitive, unclassified information (that is, personal information such as Social Security numbers).

We were granted the ability to access and read information in the Access Control Facility 2 security software. All testing of systems and security software was performed in a controlled environment with management's approval. Based on those tests, we concluded that the data reviewed were sufficiently reliable to achieve the audit objectives and support the audit conclusions.

Review Period and Standards. We performed this financial-related audit from October 1996 through November 1997 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. Accordingly, we included tests of management controls considered necessary.

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

Management Control Program

DoD Directive 5010.38, "Management Control Program," August 26, 1996, 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. The scope of review of the management control program included reviews on the adequacy of management and security controls over the Retiree and Casualty Pay Subsystem. Specifically, the review evaluated DFAS management controls over establishment of a security program, access controls, software development and change controls, segregation of duties, system software controls, and service continuity. Also, the review evaluated the results of the DFAS Cleveland Center's self-evaluation of those management and security controls during FY 1994 through FY 1996 and its annual statement of assurance.

Adequacy of Management Controls. We identified a material management control weakness as defined by DoD Directive 5010.38. The DFAS Cleveland Center's security controls over the Retiree and Casualty Pay Subsystem could be improved. Specifically, improvements were needed in monitoring and updating the security program, controls over access to the Subsystem, and providing for continuity of operations.

Six prior audits on DFAS have reported the need for similar improvements as discussed in this report. The repeat occurrence of these conditions suggests that a material weakness in security controls for information systems may exist throughout DFAS. (See Appendix B for a summary of prior audit coverage).

The recommendations in this report, if implemented, will improve security controls over the Retiree and Casualty Pay Subsystem. A copy of the report will be provided to the senior official responsible for management controls at the DFAS Cleveland Center.

Adequacy of Management's Self-Evaluation. The DFAS Cleveland Center had conducted a self-evaluation on June 9, 1994, of the security controls on the Retiree and Casualty Pay Subsystem. The self-evaluation correctly identified the risk associated with the program as high. However, in its evaluation, the DFAS Cleveland Center did not identify the specific material management control weakness identified by the audit. Further, the evaluation should have been updated, when significant changes occurred, since it was a high risk area.

Appendix B. Summary of Prior Coverage

Six Inspector General, DoD, reports covered issues related to this audit.

IG, DoD, Report No. 97-052, "Vendor Payments-Operation Mongoose, Fort Belvoir Defense Accounting Office and Rome Operating Location," December 23, 1996. The report concludes that management of security over payment data at the DFAS Operating Location at Rome, New York, did not comply with DoD security policy. As a result, unauthorized users could compromise or manipulate data without risk of detection. DFAS concurred with the recommendations and stated that it would:

- o assign a minimum number of individuals to maintain the password file and the security table;

- o establish procedures to remove terminated employees' from the Computerized Accounts Payable System;

- o discontinue allowing users to both input and certify disbursement transactions;

- o distribute user access listings to supervisors each month to verify access rights; and

- o develop and implement a contingency plan to recover computer records in the event of a disaster.

IG, DoD, Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996. The results in the report are summarized below.

- o User access to the military pay system at the DFAS centers in Denver, Colorado, and Indianapolis, Indiana, was not adequately controlled and limited. Therefore, resources were not secure and the integrity of pay data for Army and Air Force servicemembers was at risk.

- o Responsibilities for authorizing and controlling access to the military pay system were not clearly defined and understood at one center and two supporting organizations. Accordingly, access to the pay system and sensitive Army and Air Force pay data was improperly attained and security oversight was inadequate.

- o Administrative controls over the security of the pay system at the two centers and three supporting organizations needed improvement. As a result, the integrity of the military pay data was vulnerable.

The report recommended that reviews be conducted at the two centers to ensure that user access was properly controlled and limited; improvements were made in defining responsibilities for authorizing and controlling access to the military pay system; security administrator positions were established with appropriate

Appendix B. Summary of Prior Coverage

authority and oversight capabilities; and organizations were required to identify and control all critical-sensitive positions.

The Defense Information Systems Agency and DFAS concurred with the findings and recommendations.

IG, DoD, Report No. 96-124, "Selected General Controls Over the Defense Business Management System," May 21, 1996. The report states that computer security at the Defense Finance and Accounting Service Financial Systems Activity in Columbus, Ohio, did not adequately protect the Defense Business Management System development code from compromise. Also, the Financial Systems Activity did not adequately control program software changes to ensure that only authorized changes were made.

As a result, these general control weaknesses compromised the reliability of the Defense Business Operations Fund financial statements. These weaknesses also increased the risk of fraud, sabotage, and disruption to the operations of the DoD Components that rely on the Defense Business Management System.

The Defense Finance and Accounting Service concurred with recommendations made concerning computer security; software change management practices (except for a review of the existing software code); and disaster preparedness. The Defense Information Systems Agency concurred with the recommendations to complete, finalize, and test the disaster recovery plan.

The Defense Logistics Agency agreed to update their disaster recovery plan but delayed performing a disaster recovery risk analysis until it could determine a new location for its computer laboratory. Also, the Defense Logistics Agency agreed with periodic testing of its disaster recovery plan.

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. The related report states that two Defense megacenters--Defense Megacenter, Saint Louis, Missouri, and Defense Megacenter, Denver, Colorado--had made commendable efforts to implement 22 of the 25 prior audit recommendations.

At the Defense Megacenter, Denver, Colorado, the planned corrective actions on the remaining three recommendations were considered adequate, although incomplete. However, a new security software problem was identified during the audit that required corrective action by the Defense Information Systems Agency, Western Hemisphere at Fort Ritchie, Maryland.

The Defense Information Systems Agency, Western Hemisphere and the Defense Megacenter, Denver, Colorado, concurred with all recommendations to complete corrective actions from prior audit reports.

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. The report states that the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency made commendable efforts to implement prior audit recommendations.

However, additional corrective actions were required in some areas. The review followed up on 87 of the 112 recommendations made in prior audit reports. Audit followup on 25 recommendations was deferred because the organizations to which the recommendations were made were being consolidated into various Defense Information Systems Agency megacenters.

Of the 87 recommendations, the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency had taken adequate corrective actions on 67 recommendations. Additional corrective actions were required on 20 recommendations.

The Defense Finance and Accounting Service and its Financial Systems Activity at Denver concurred with the recommendations to improve physical security at one Defense megacenter and to eliminate a security exposure on one system. The Defense Information Systems Agency concurred with 11 recommendations and partially concurred with 3 recommendations to improve computer security, operational efficiency, and management controls at computer centers.

The Defense Logistics Agency concurred with all recommendations and stated that it would develop and implement controls over supervisor calls (with integrity exposures); export corrected supervisor calls to the Defense Megacenter at Columbus, Ohio; and finalize procedures for managing the processing and exporting of changes to its operating system.

IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. The report states that the Defense Business Management System's users neglected to change their passwords within 180 days. In addition, numerous users had not changed their passwords in over 1 year.

These conditions had occurred because security personnel at the Defense Information Services Organization-Columbus Center did not periodically review the age of passwords nor deny access to users whose passwords had not been changed in 180 days. The report recommended that employees be automatically required to change their passwords every 90 days. The Defense Information Services Organization concurred with the recommendation and stated that it would install an automated password change facility that would force users to change their passwords every 90 days.

Appendix C. Major Categories of General Controls

We evaluated six major categories of general controls. Those categories included the security program, access controls, software development and change controls, duty segregation, system software controls, and service continuity.

Security Program. The security program should provide a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the organization's computer-related controls.

Access Controls. Access controls limit or detect access to computer resources (such as data, equipment, and facilities) thereby protecting the resources against unauthorized modification, loss, and disclosure.

Software Development and Change Controls. Software development and change controls prevent unauthorized programs or modifications to an existing program from being implemented.

Duty Segregation. Duty segregation includes policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

System Software Controls. System software controls limit and monitor access to the powerful programs and sensitive files that control the computer equipment and secure computer programs supported by the system.

Service Continuity. Service continuity controls ensure that, when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

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 Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Finance and Accounting Service Cleveland Center
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Appendix D. Report Distribution

Non-Defense Federal Organizations

Office of Management and Budget
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 Government Management, Information, and Technology,
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

Part III - Management Comments

Defense Finance and Accounting Service Comments



DFAS-HQ/FMM

DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

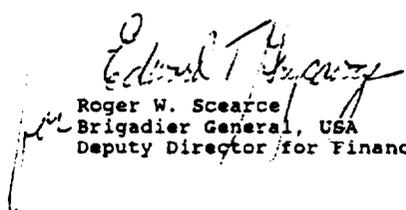
JAN 28 1998

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE,
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: DoD IG Draft Report, "Selected General Controls
Over the Retiree and Casualty Pay Subsystem at
the Defense Finance and Accounting Service-
Cleveland Center," dated November 1, 1997
(Project 6FG-0093)

The comments to the findings and recommendations
documented in the subject draft report are included as
attachments to this memorandum.

My point of contact is Patricia McGriff, DFAS-HQ/FMM,
(703) 607-5062.


Roger W. Scarce
Brigadier General, USA
Deputy Director for Finance

Attachments:
As stated

Recommendation 1: The Defense Finance and Accounting Service - Cleveland Center update the risk assessment and the security plans to reflect current facilities, operations, and risks. The plan should be updated when significant changes occur in facilities, operations, or risks.

DFAS-CL Response: Concur.

DFAS-CL Comments: The Cleveland Center is currently in the process of certifying and accrediting all DFAS-CL systems including the Retiree and Casualty Pay Subsystem (RCPS). The Certification and Accreditation (C&A) process for the Defense Retiree and Annuitant Pay System (DRAS), of which RCPS is a part, is about one third complete. Once the C&A is completed, documents will be reviewed annually, or if significant changes occur, such as the proposed Defense Information Systems Agency (DISA) move of Defense Megacenters (DMCs) scheduled for mid-1998. The operations for RCPS are targeted to move from DMC Chambersburg (DMC-C) to DMC Mechanicsburg (DMC-M) in mid-1998.

Estimated Completion Date: March 31, 1998.

Recommendation 2: The Defense Finance and Accounting Service - Cleveland Center evaluate the training and experience of personnel prior to their selection for security related responsibilities to ensure that candidates have the minimum security training and experience qualifications.

DFAS-CL Response: Concur.

DFAS-CL Comments: The Cleveland Center is currently in the process of restructuring its Information System Security Officer (ISSO) and Terminal Area Security Officer (TASO) positions. There will be one ISSO for each system owned by DFAS-CL. The TASO position will be responsible for system access control. ISSO and TASO positions for the RCPS will be filled based on selection criteria provided by DFAS-CL's Information Security Office (ISO). The selection criteria utilized is in accordance with the requirements of the National Computer Security Center's "A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems." The selection criteria includes: two years of experience in a computer related field, familiarization with the operating system of RCPS, good management skills and the ability to deal with all levels of personnel from top management to individual users. It is expected that the Designated Approving Authority (DAA) will issue the official ISSO/TASO appointment letters sometime in January 1998, after the required background investigations have been performed. The DFAS-CL Information Security Office staff will conduct computer security training after the official appointments are announced by the DAA.

Estimated Completion Date: March 31, 1998.

Recommendation 3: The Defense Finance and Accounting Service - Cleveland Center review sensitivity levels of security personnel positions and require appropriate background investigations before assigning personnel to security positions.

DFAS-CL Response: Concur.

DFAS-CL Comments: Sensitivity levels of security personnel positions will be reviewed by the Security Office, DFAS-CL Plans and Management Directorate in conjunction with the restructuring program for the ISSO and TASSO positions. In cases where the appropriate investigation has not been conducted, action will be taken to initiate the investigation.

It is the employing management's responsibility to complete the DFAS Form 113, "Position Designation Record." It is the responsibility of the Customer Support Unit (CSU) of the Human Resources Office to ensure that one is on record for each position. The DFAS Form 113 identifies the sensitivity of the position and should be completed when a position is created or when there are changes to the duties that call for a different sensitivity. This will be an ongoing process.

Prior to occupancy of a position, the DFAS Form 114, "Pre-Appointment Investigative Requirement Check," should be processed (from the CSU to the Security Office and return) to ensure the appropriate investigative requirements are met for the position being occupied. This will be an ongoing process.

Additionally, request clarification of the following information provided in the DoD IG Draft Report, page 7 under "Levels of Security Clearances."

The first paragraph, refers to the levels of security clearances not being reviewed prior to assignment and mentions the DoD 5200.2-R requirement that each civilian position be classified as critical sensitive, noncritical sensitive or nonsensitive. This indicates the positions have not been designated. Yet, the remainder of the section seemingly refers to inaccurate designations - an indication the positions have been designated but the DoD IG disagrees with the designation.

Paragraph three of the same section, states the assistant information security officer's (AISO) position should be designated critical sensitive because in the absence of the information security officer those duties would be assumed by the AISO. Request the basis for this requirement.

Estimated Completion Date: March 31, 1998

Recommendation 4: The Defense Finance and Accounting Service - Cleveland Center correct any deficiencies that can prevent the accreditation of the retired pay subsystem. Conduct re-accreditations when significant changes occur.

DFAS-CL Response: Concur.

DFAS-CL Comments: The re-accreditation program for the RCPS is currently in process. The initial 3 phases of the accreditation program are scheduled to be completed by January 31, 1998. The remaining phases of the program will be completed by the second quarter of FY 1998.

Estimated Completion Date: March 31, 1998.

Recommendation 5: The Defense Finance and Accounting Service - Cleveland Center monitor accesses to the system and investigate unusual use of the system.

DFAS-CL Response: Concur.

DFAS-CL Comments: The Access Control Facility 2 (ACF2), which is the security platform for RCPS at DMC-C, generates daily reports to help monitor user access to RCPS. DMC-C regularly monitors the daily reports to determine if there have been attempts by unauthorized users to access the system. DFAS-CL would be notified if unauthorized usage of the system does appear on the ACF2 reports. DFAS-CL was informed during recent discussions with DMC-C that there has been no unusual or unauthorized use of the RCPS system. Additionally, DMC-C informed DFAS-CL how to access the ACF2 daily reports and DFAS-CL is now developing procedures to monitor these reports on a regular basis. Once the new procedures are in place both DFAS-CL and DMC-C will be monitoring the daily reports. Participation by both organizations will have the effect of a dual internal control. The procedures are targeted to be in place by the end of February 1998.

Estimated Completion Date: February 28, 1998.

Recommendation 6: The Defense Finance and Accounting Service - Cleveland Center limit access to offices and computer equipment in the Federal Building.

DFAS-CL Response: Concur (Action Completed).

DFAS-CL Comments: DFAS-CL is a tenant in the A.J. Celebrezze Federal Building (FOB), located in Cleveland, Ohio. Access to the FOB is controlled and monitored by the Federal Protective Service (FPS). Upon entrance to the FOB non-DoD visitors are required to go through a metal detector device and are also subject to a body scan by electronic baton. At the end of the day, doors are locked by the last employee departing the work area and the FPS also conducts floor patrols to ensure doors are locked. Additionally, DFAS-CL employees are constantly briefed on security awareness issues by attending periodic meetings on security and also by electronic messages posted on the E-mail bulletin board.

In addition to the general FOB safeguards described above, other physical and electronic controls are in place. These include: the issuance and personal display of the DFAS-CL security ID badge by Center employees, required DoD badges for entrance into the building, cipher locks installed on computer room doors to ensure unauthorized access is denied, and password protected computer systems to ensure against unauthorized system access

Estimated Completion Date: Action completed.

Recommendation 7: The Defense Finance and Accounting Service - Cleveland Center identify office space and equipment needed to support critical operations at an alternate site in the event of a disaster.

DFAS-CL Response: Concur (Action Completed)

DFAS-CL Comments: DFAS-CL already has a Continuity of Operations Plan (COOP) and a Living Disaster Recovery Plan System (LDRPS). Within these plans it specifically identifies and lists essential equipment needed for DFAS-CL to continue critical operations. DFAS-CL does not specifically identify or secure office space until the need is identified based upon the emergency or disaster. However, space alternatives are available depending upon the emergency space requirements.

If the need is partial or a small block of space is needed, DFAS-CL would try to accommodate itself internally by utilizing other areas within the DFAS-CL allotted office space. This would include the North Point operation which is a facility separate from the FOB. If DFAS-CL could not meet its needs in this manner, the General Services Administration would be called upon to provide additional space within the FOB. In the event DFAS-CL operations were completely destroyed, other alternatives would be pursued. Other DFAS Centers and OPLOCs would be called upon to see what assistance could be offered. As a second alternative DFAS-CL would look to other government

5

agencies for help and as a third alternative DFAS-CL would work with the GSA Chicago Region to find suitable local office space to meet our needs.

Estimated Completion Date: Action completed.

Recommendation 8: The Defense Finance and Accounting Service - Cleveland Center conduct periodic reviews and correct any identified deficiencies in the security controls over the Retiree and Casualty Pay Subsystem.

DFAS-CL Response: Concur.

DFAS-CL Comments: DFAS-CL is already pursuing corrective action in regard to this recommendation. Please see the DFAS-CL comments for recommendation #5.

Estimated Completion Date: February 23, 1998.

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

**F. Jay Lane
Kimberley A. Caprio
Dennis L. Conway
Cynthia G. Williams
Marcia L. Ukleya
Deborah Curry
Traci Y. Sadler**

