Audit

Report

COMPUTER SECURITY FOR
THE DEFENSE CIVILIAN PAY SYSTEM

Report No. 99-107 March 16, 1999

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 Audit Followup 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 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 22202-2884

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, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AIS	Automated Information System
CA-ACF2	Computer Associates International, Inc., Access Control Facility 2
DAA	Designated Approving Authority
DCPS	Defense Civilian Pay System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DMC	Defense Megacenter
FSA	Financial Systems Activity
FSO	Financial Systems Organization
ISSO	Information System Security Officer

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

March 16, 1999

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

SUBJECT: Audit Report on Computer Security for the Defense Civilian Pay System (Report No. 99-107)

We are providing this report for review and comment. This report is one in a series of reports on security software and application controls over the Defense Civilian Pay System. We considered management comments on a draft of this report in preparing the final report.

Comments from the Defense Information Systems Agency were fully responsive. Comments from the Defense Finance and Accounting Service were partially responsive. We request additional comments from the Defense Finance and Accounting Service by May 16, 1999. Specific requests for additional management comments are stated in Part I of the report.

We appreciate the courtesies extended to the audit staff Questions on the audit should be directed to Mr. Brian M. Flynn, at (703) 604-9145 (DSN 664-9145), e-mail BFlynn@dodig.osd.mil, or Mr. W. Andy Cooley, (303) 676-7393 (DSN 926-7393), e-mail WCooley@dodig.osd.mil. See Appendix B for the report distribution. The audit team members are listed inside the back cover.

Robert J Lieberman

Robert J. Lieberman
Assistant Inspector General
for Audit

Office of the Inspector General, DoD

Report No. 99-107 March 16, 1999
(Project No. 7FD-2023)

Computer Security for the Defense Civilian Pay System

Executive Summary

Introduction. This audit is one in a series of audits focused on security software controls for the civilian pay application known as the Defense Civilian Pay System. In FY 1991, the Defense Civilian Pay System was approved as the migratory civilian pay system for the Department of Defense. The application currently services approximately 700,000 employees and processes more than $35 billion in payroll transactions. Employee pay records and account data are serviced by the Defense Finance and Accounting Service Denver Center, Denver, Colorado, and Defense Finance and Accounting Service Operating Locations in Charleston, South Carolina, and Pensacola, Florida. Computer programming support was provided by the Defense Finance and Accounting Service, Financial Systems Organization, Financial Systems Activity, Pensacola. The Defense Information Systems Agency, Defense Megacenter, Mechanicsburg, Pennsylvania, and the Systems Support Office, Dayton, Ohio, provided computer support for the pay data serviced by the Defense Finance and Accounting Service.

Audit Objectives. The primary audit objective was to determine whether security software controls over the Defense Civilian Pay System adequately safeguarded the data integrity of employee payroll records. The review of the management control program applicable to the other stated audit objective will be discussed as part of a later report.

Audit Results. Computer security over the Defense Civilian Pay System application needed improvement.

- The Information System Security Officer appointed for the civilian pay application did not have the authority, system access, or training necessary to enforce security policies and safeguards on all personnel with access to the pay application.

- Security was not uniformly implemented for other key Defense Finance and Accounting Service financial applications.

- The sensitive security privilege on the civilian pay production platform located at the Defense Information Systems Agency, Defense Megacenter, Mechanicsburg, was not adequately restricted to security personnel within the Defense Information Systems Agency.

No instances of fraud or abuse were detected. However, computer security controls must be strengthened to ensure the integrity of the civilian pay data and the protection of Federal information assets. For details of the audit results, see Part I of the report.

Summary of Recommendations. We recommend that the Defense Finance and Accounting Service appoint qualified personnel as Information System Security Officers and include the functional responsibilities mandated by a DoD directive in the position descriptions for these security positions. In addition, we recommend that specific instructions be incorporated in regulation to ensure that the security officers are adequately trained, given the authority and responsibility commensurate with their functional requirements, and placed at the highest level within the organization to ensure independence from the operational elements of the organization. We also recommend that the sensitive security administrative authority be restricted to the Defense Information Systems Agency personnel responsible for computer mainframe maintenance and support.

Management Comments. The Defense Finance and Accounting Service concurred or partially concurred with the recommendations. The Defense Finance and Accounting Service stated that responsibilities and minimum qualification standards, including training requirements, for Information System Security Officers will be defined in their security regulation. Management will request that security responsibilities be incorporated into position descriptions and will clarify segregation of duties in their security regulation. Annual security compliance reviews will be required to ensure that qualified personnel are appointed to security positions and that these personnel have the training and system access necessary to perform their duties.

The Defense Finance and Accounting Service partially concurred with the recommendation to define the operational element of each system because to do so would be unnecessary and impractical. Management stated that its ability to appoint the best qualified personnel to security positions would be impeded by implementing the audit recommendations to establish a specific chain-of-command and reporting structure for all Information System Security Officers (including direct line authority over security administrators) and to ensure the independence of security officers from operational elements. As an alternative, the reporting structure and working relationships among the security officers and the principal managers of the applications will be clarified in the Defense Finance and Accounting Service regulation. The Defense Information Systems Agency concurred with the recommendation to review and restrict all sensitive administrative authority to the civilian pay systems.

Audit Response. We consider the Defense Finance and Accounting Service comments fully responsive on three recommendations and partially responsive on four recommendations. The Defense Finance and Accounting Service should confirm that all Information System Security Officers are in compliance with minimum qualification and training requirements. We disagreed with Defense Finance and Accounting Service comments on defining the operational elements of each system, clarifying the roles and responsibilities of security officers and defining a proper chain-of-command for security officers. Defining the operational elements of each system is essential for establishing a security structure baseline and ensuring the independence of the security function. Clarifying the roles and responsibilities of the security officers will not be sufficient to ensure they are accountable for and actively involved in day-to-day security administration. The chain-of-command for the security function should be specifically defined to enable the security officers to execute the requirements of the security position as mandated by DoD directive. We request that management reconsider its position on those recommendations.

See Part I for management comments and audit responses and Part III for the complete text of management comments. We request that the Defense Finance and Accounting Service provide comments on this report by May 16, 1999.

Table of Contents

Part I - Audit Results

Audit Background

System Overview. The Defense Civilian Pay System (DCPS) was approved by the Under Secretary of Defense (Comptroller) as the DoD migratory civilian pay system in September 1991. The primary objective of DCPS is to standardize DoD civilian pay and to fulfill all pay-related reporting requirements. To accomplish this, DCPS maintains employee records that contain pay and leave entitlements, deductions, withholdings, time and attendance data, and all other information pertinent to an employee's employment status. DCPS users consist of the Military Departments, the Defense Finance and Accounting Service (DFAS), and other organizations in the Federal Government. DCPS currently services approximately 733,000 payroll accounts and processes payroll transactions valued at more than $38 billion annually. DCPS was fully implemented in June 1998.

Supporting Organizations. Support for the DCPS application and mainframe computers is provided by four DFAS organizations and the Defense Information Systems Agency (DISA).

DFAS Financial Systems Activity. Software development, design, testing, and other central design support for the DCPS application is provided by the DFAS Financial Systems Organization (FSO), Financial Systems Activity (FSA), at Pensacola, Florida (DFAS FSA Pensacola).

DFAS Payroll Offices. The payroll office at the DFAS Denver Center, Denver, Colorado, and DFAS Operating Locations in Charleston, South Carolina, and in Pensacola maintain employee pay records and DCPS account data.

DISA. The DCPS application resides on separate mainframe computers located at the Defense Megacenters (DMCs) in Mechanicsburg, Pennsylvania, and in Denver.

- The DCPS production environment (the WCC[1]) at the DMC Mechanicsburg supports the employee account data maintained by the DFAS Operating Locations in Charleston and Pensacola. DMC Mechanicsburg provides executive software support for this environment.

- The DCPS employee account data maintained by the DFAS Denver Center reside on a mainframe computer located at the DMC Denver. However, the DISA Systems Support Office (SSO), Dayton, Ohio, provides executive software support for the processing environment, which is known as the CP1.

Security Software. Computer Associates International, Inc., Access Control Facility 2 (CA-ACF2) is the external security software used to protect the CP1 and WCC processing environments. CA-ACF2 provides system security and control

[1] WCC is used in this report as an identifier for the DCPS production platform at DMC Mechanicsburg.

over DCPS software, data, and data communications. It identifies the users who have access to the computer systems and defines the resources that the users are authorized to access. When properly implemented, CA-ACF2 ensures that the operating system and application software are protected according to DoD security requirements.

Chief Financial Officers Act of 1990. This audit supports the financial statement audit requirements of Public Law 101-576, the "Chief Financial Officers Act of 1990," November 15, 1990, as amended by Public Law 103-356, the "Federal Financial Management Act of 1994," October 13, 1994. The civilian pay data were reported in the "Department of Defense Agency-wide Financial Statements for FY 1997 Financial Activity, Statement of Operations and Changes in Net Position." Footnote 23 to line item 9, Program or Operating Expenses, lists the actual pay data as "Personal Services and Benefits." DCPS summarizes the total amount paid by each paying office and reports the figures to the appropriate payroll office on the 592 Disbursement Report. The pay data are entered into more than 40 different accounting systems that report the totals through accounting offices to the financial statements.

Audit Objectives

The primary objective of our audit was to determine whether the security software controls adequately safeguarded the integrity of DCPS pay data. Although an evaluation of the effectiveness of applicable management controls was an announced objective, we did not perform an evaluation during this audit. A later report will discuss the management control program.

See Appendix A for a discussion of the scope and methodology and a discussion of prior audits related to our audit objectives.

Adequacy of Security Controls

Security controls over the DCPS application and other key financial applications within DFAS needed improvement.

- DFAS FSA Pensacola designated an individual as the DCPS Information System Security Officer (ISSO) when the person did not have the training, authority, or system access necessary to adequately enforce security policies and safeguards on all personnel with access to the application.

- DFAS did not uniformly implement security on other key financial applications throughout the organization.

In addition, the sensitive security privilege was not adequately restricted to DISA Dayton Systems Support Office personnel on the DCPS CP1 computer mainframe platform.

Inadequate guidance issued by DFAS resulted in problems with the DCPS ISSO at DFAS FSA Pensacola and inconsistent security implementation within DFAS. The Dayton Systems Support Office did not review and limit DFAS FSA Pensacola personnel to DCPS resources when CP1 computer mainframe support responsibilities transferred to DISA. We did not find instances of unauthorized access or unauthorized software modifications. However, security controls over the DCPS data and the supporting computer production environments must be strengthened to ensure the integrity of the civilian pay data and protect Federal information assets.

Security Guidance

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, mandates minimum AIS security requirements within the DoD. Additional guidance for meeting the DoD requirements is provided in a series of documents by the National Security Agency, National Computer Security Center. Although not required by the DoD Directive, DFAS should consider the information that the National Security Computer Center provides as a baseline for use in building a security infrastructure within the DFAS organization. DFAS Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," Version 4, August 21, 1996 (the DFAS Regulation), provides instructions for implementing the DoD Directive throughout DFAS.

DoD Directive. The Directive requires the Heads of DoD Components to:

> Implement an AIS security program designed to ensure compliance with this Directive. . . . Assign official(s) as the DAA [Designated Approving Authority] (e.g., senior AIS policy official) responsible for . . . ensuring compliance with AIS security requirements.

Specific DAA responsibilities include ensuring that an ISSO is named for each AIS and that the ISSO receives training required to perform the duties of the function.

The ISSO should not report to operational elements of the AIS over which security requirements must be enforced. The ISSO will have security responsibility and authority for the AIS. Specifically, each ISSO must:

- ensure that the AIS is maintained and disposed of in accordance with internal security policies and practices;
- have the authority to enforce security policies and safeguards on all users who have access to the AIS for which the ISSO is responsible, and
- ensure that users have the required personnel security clearances, authorization, and need-to-know.

The DAA for the DCPS application was the Deputy Director of the DFAS Information Management Deputate. The ISSO assigned to the DFAS FSA Pensacola was responsible for securing DCPS application resources on the production platforms at the Defense megacenters in Denver and Mechanicsburg.

National Computer Security Center Guidance. The National Computer Security Center guide, "A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems," May 1992 (the Security Center Guide), identifies and suggests the minimum qualifications for ISSOs and offers a more in-depth explanation of the importance of the ISSO role based on industry-accepted standards. The guide also discusses the roles and responsibilities of other individuals responsible for security and their relationship to the ISSO. DFAS should consider information provided in the Security Center Guide in designing a security infrastructure that complies with the requirements of the DoD Directive.

DFAS Regulation. DFAS Regulation 8000.1-R provides instructions for implementing DoD Directive 5200.28 throughout DFAS. The DFAS Regulation provides definitive guidance in some areas of security administration. However, the Regulation does not provide adequate clarification on the security chain-of-command and alignment of security roles, responsibilities, and relationships necessary to:

- strengthen security controls,
- achieve uniform application and implementation of security policy throughout DFAS, and
- comply with the requirements of the DoD Directive.

Deficiencies in security policies and procedures increase the risk of unauthorized access, data manipulation, fraud, waste, and abuse of Federal information assets.

DCPS Security

Security control over the DCPS application was the responsibility of the appointed ISSO at DFAS FSA Pensacola. Although security administration was performed by personnel within the organization, the ISSO position itself remained vacant from September 1996 through October 1997. When we brought the condition to management's attention, the DCPS Program Manager immediately appointed an ISSO using the DFAS Regulation as a guide. However, the individual placed in the ISSO position did not have the technical security training, system access, or authority necessary to enforce security policies and safeguards on all personnel with access to the DCPS application as mandated by the DoD Directive.

- The ISSO was not trained on the technical aspects of CA-ACF2, the external security software used to protect the DCPS application. As a result, the ISSO did not possess the specific technical knowledge and skills necessary to adequately review audit files and user access permissions. Rather, the ISSO relied on the knowledge and skills of other DFAS FSA Pensacola personnel to provide the information necessary to satisfy these requirements. DCPS users include not only personnel at the DFAS FSA Pensacola, but also payroll offices and activities throughout the world. To monitor and control these user access permissions, it is imperative that the ISSO possess the technical knowledge of CA-ACF2 in order to understand where the user information is; how it is maintained and controlled; and how to request and retrieve the specific information desired. Without the knowledge and capability to request and retrieve this information personally, the ISSO is not assured that the information is complete and accurate. Likewise, knowledge of CA-ACF2 is necessary to understand and interpret the resulting security reports.
- The ISSO did not have the system access capability necessary to monitor or administer security control over all users to the CP1 and WCC DCPS production platforms as mandated by the DoD Directive.

This capability, linked with the necessary technical training on CA-ACF2, is vital to ensure the DCPS user community is limited to valid users with a need to know.

- The ISSO did not have direct line of authority over the DFAS FSA Pensacola staff performing the day-to-day security functions for the DCPS application. Thus, the authority and control of the ISSO over the daily accomplishment of security administration and oversight were diminished. Specifically, the appointed ISSO was the Director of the Software Engineering Division, while the DFAS FSA Pensacola staff performing the day-to-day security functions was supervised by the Chief, Project Support Branch, within the Project Support Division. The DFAS FSA Pensacola security structure included a "dotted line" that allegedly gave the ISSO authority over these staff members for security related issues. In effect, this "dotted line" security structure permitted the ISSO to circumvent the direct supervisory authority of the Director, Project Support Division, and the Chief, Project Support Branch, over these staff members for all security related issues.

The DFAS Regulation does not provide adequate guidance to ensure that individuals appointed to ISSO security positions have the authority, knowledge, and skills commensurate with the ISSO functional responsibilities mandated by the DoD Directive. Without adequate security policies and procedures, the integrity of the DCPS data is at risk of unauthorized access or modification, fraud, waste, and abuse.

DFAS Security Implementation

DFAS did not uniformly implement security over the DCPS application and other key DFAS financial applications. The DFAS Regulation did not provide adequate guidance to achieve uniform implementation of security policy throughout DFAS and did not ensure appropriate assignment of security responsibilities. Consequently, DFAS did not ensure that ISSOs were appointed, trained, and granted the authority to maintain the AIS and enforce security policies and safeguards on all AIS users.

ISSO Appointment. DFAS did not ensure that it assigned a primary ISSO to each DFAS AIS, that authorized personnel signed appointment letters, or that the ISSOs appointed were the individuals actually doing the day-to-day security functions.

- As detailed in Appendix A, the Inspector General, DoD, Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996, determined that the DFAS Indianapolis Director of Military Pay did not establish an ISSO.

- The DFAS Cleveland Center did not assign a primary ISSO for the Defense Joint Military Pay System and other applications, but rather ISSO functions were dispersed among several individuals within the AIS operational elements.

- The DAAs at the DFAS Denver and Cleveland Centers signed blanket appointment letters that inappropriately included the appointment of ISSOs for systems at the DFAS-level over which they had no authority.

- The appointed ISSO for the DCPS application did not perform the daily security administration for the DCPS application. Rather, individuals assigned elsewhere within the DFAS FSA Pensacola performed security administration.

- The appointed ISSO for the annuity pay application at the DFAS Denver Center did not perform daily security administration for the application. Instead, individuals assigned elsewhere within the Directorate of Annuity Pay accomplished the responsibility.

ISSO Qualifications. To ensure the integrity of AIS data, DFAS must also ensure that individuals appointed to the ISSO positions have the technical background necessary to enable them to accomplish the functional requirements of the position as mandated by the DoD Directive. The Security Center Guide recommends that the ISSO possess a technical degree in computer science, mathematics, electrical engineering, or a related field. The minimum ISSO qualifications recommended by the Security Center Guide are:

- 2 years' experience in a computer-related field,

- 1 year of computer security experience or mandatory computer security training, and

- familiarization with the AIS operating system.

DFAS did not provide guidance on the required qualifications for the ISSO position. In addition, the functional responsibilities mandated by the DoD Directive were not included in the ISSO position descriptions. Per discussions with representatives from the Human Resource Directorates at the DFAS Denver and Indianapolis Centers, position descriptions must include all duties and responsibilities if the amount of time required to perform these duties exceeds 25 percent. In addition, all major duties described in a position description must total 100 percent. Based on the size of the pay applications, the magnitude of the user community over which security rules must be enforced, and the high risk for potential exposure to these applications, the ISSO responsibilities would require more than the 25 percent minimum for inclusion in the ISSO position descriptions

- The position descriptions for the DCPS and the Navy Defense Joint Military Pay System ISSOs did not include ISSO security responsibilities required by the DoD Directive. However, DFAS Cleveland Center outlined the responsibilities of the Navy military pay ISSO in an attachment to the ISSO position description.

- Although the position descriptions for the appointed ISSOs for the Air Force and Army Defense Joint Military Pay System included security responsibilities as the primary function of the position, the position descriptions did not address or include all of the responsibilities mandated by the DoD Directive.

DFAS should consider the minimum qualifications when appointing personnel to an ISSO position. To ensure that the DoD Directive requirements are met, the ISSO functional responsibilities should be incorporated into the position descriptions for these personnel.

ISSO Training. The DAA should ensure that the ISSO receives applicable training to carry out the duties of the function. In implementing the requirement, the DFAS Regulation states that the DAA is to ensure that an AIS training program is in place, to include specialized training for AIS security staff. However, the DFAS Regulation does not provide definitive guidance on specific training requirements commensurate with security responsibilities. As a result, DFAS could not ensure that security officers had the necessary knowledge and skills required to perform their security functions.

- The individual selected as the DCPS ISSO was not trained on the technical aspects of the CA-ACF2 security software used to protect the DCPS application data and to control user access.

- The appointed ISSO for the annuity pay application at the DFAS Denver Center did not have the specific training necessary to perform the functional requirements of the ISSO position.

Segregation of Duties. Segregation of duties is an important element of the system of internal control for every application. Both industry standards and good prudent business practices dictate specific segregation between duties performed within the data center environment. For example, the Institute of Internal Auditors Research Foundation, "Systems Auditability and Control Report," Module 4, "Managing Computer Resources," states that different persons should be selected to perform the functions of systems software maintenance and data security. Regardless of the industry standards suggested by the Internal Auditors Research Foundation and other reliable sources, both the data security and software development and maintenance functions for the DCPS application were performed by the DFAS FSA Pensacola. Specifically, the ISSO for the DCPS application was also the Director for the Software Engineering Division responsible for designing the technical system architecture and software for DCPS as well as testing and evaluating the application modules. The DFAS Regulation does not provide instruction for separating these conflicting duties. This segregation is essential for DFAS to maintain a good internal control structure for DCPS and other DFAS applications.

Security Reporting Structure. The DoD Directive recommends that "the ISSO not report to operational elements of the AIS over which security requirements of the directive must be enforced." The Security Center Guide reinforces the recommendation by stating that the ISSO should report to "a high level authority who is not the operational manager." Although the DFAS Regulation recognizes the ISSO as the "senior security person," it does not define the specific chain-of-command for the ISSO position or placement of the position in the DFAS organization structure. Following the lead of other organizations within the DoD, DFAS must ensure that the security function is placed within the organization structure to provide the independence and authority necessary to protect the application data. For example, DISA places the responsibility of security for the mainframe platforms at DMC Denver and DMC Mechanicsburg with separate security offices at those locations. The security officers at both megacenters have a direct chain-of-command to their Center Director.

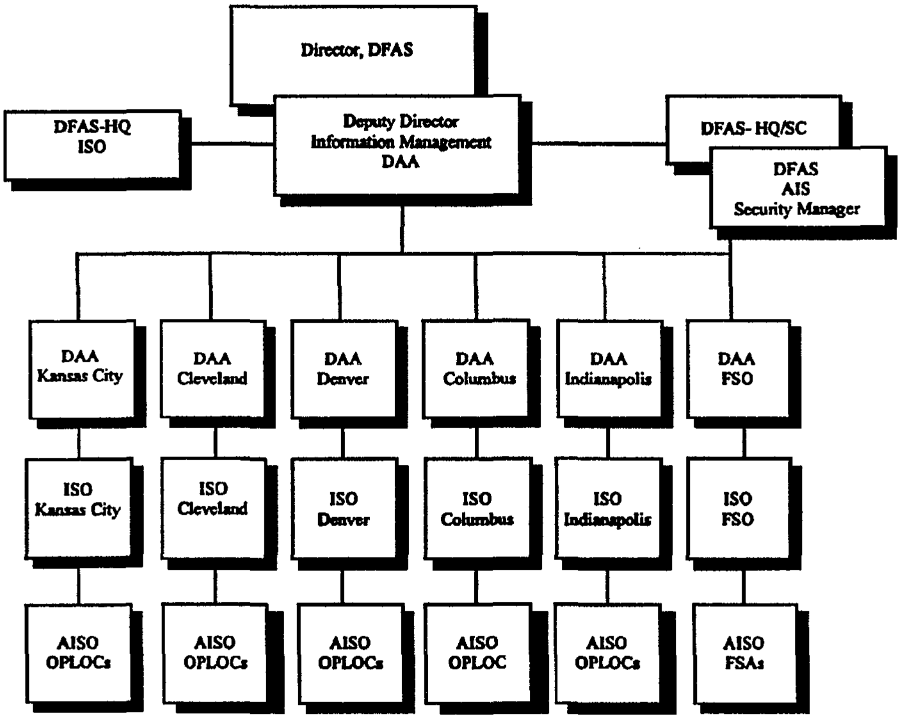
The DFAS Regulation assigns first-line responsibility for ensuring compliance with AIS security directives to the DAA, Information Security Officer, Assistant Information Security Officer, and AIS security staff, respectively. Figure 1 illustrates the DFAS AIS security organization structure in the DFAS Regulation. By not identifying the ISSO position within the structure, DFAS managers are given the flexibility to place the ISSO position anywhere within their individual organizations. Consequently, the ISSO is not uniformly positioned within DFAS, which does not ensure the independence and authority of that primary security position.

- The DCPS ISSO did not report directly to the Director, DFAS FSA Pensacola. In addition, the ISSO was not the immediate supervisor of the DFAS FSA Pensacola staff performing the day-to-day security functions for the DCPS application.

- As reported in Inspector General, DoD, Report No. 96-175, (see Appendix A), the ISSOs at DFAS Denver Center were positioned three management levels below the Director of Military Pay. As a result, the ISSOs did not have the level of authority necessary to effectively control security for Air Force pay data and application core resources. The ISSO responsible for securing Army pay data at the DFAS Indianapolis Center was positioned two management levels below the Director of Military Pay.

- The individuals performing the day-to-day security requirements of the ISSO for the DFAS annuity pay application at the DFAS Denver Center were assigned three management levels below the Director of Annuity Pay.

Figure 1 provides the intended organization structure for DFAS AIS security. However, Figure 1 does not include the chain-of-command of other positions assigned security responsibility. For example, the Information Security Officers act as the focal point for all security matters under their jurisdiction. Again, DFAS does not define the relationship between that position and the ISSO. The Information Security Officer is also responsible to the respective DAA for ensuring that security is implemented. However, the placement of the Information Security Officer within the organizational structures at the DFAS Denver and DFAS Cleveland Centers did not allow for direct reporting to their respective DAA as presented in Figure 1. Likewise, the Information Security Officer at DFAS did not report directly to the Deputy Director, Information Management, who is the DAA for DFAS AISs. Rather, two management layers exist between the DFAS Information Security Officer and the DAA.

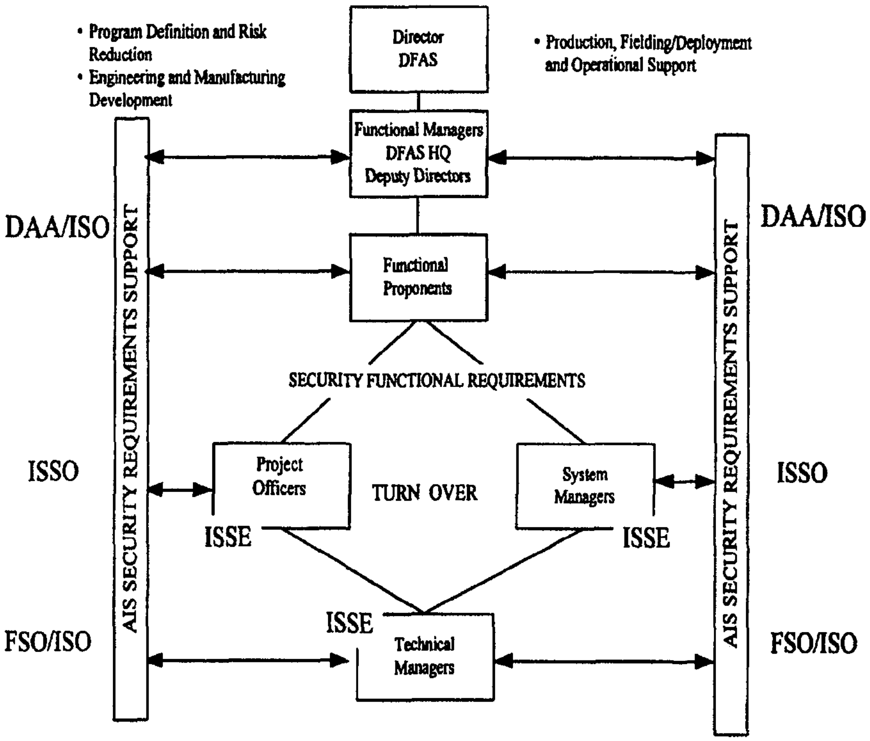


AISO	Assistant Information Security Officer
HQ	Headquarters
ISO	Information Security Officer
OPLOCs	Operating Locations
SC	Systems Evaluation and Control

Source: DFAS Regulation 8000.1-R

Figure 1. DFAS AIS Security Organization Structure

Additional undefined and inconsistent areas are apparent when considering the organizational structure in Figure 1 in association with the security relationship among DFAS functional managers. Figure 2 illustrates the DFAS Functional Managers' Relationship chart.[2]


• Program Definition and Risk Reduction
• Engineering and Manufacturing Development
Director DFAS
• Production, Fielding/Deployment and Operational Support
Functional Managers DFAS HQ Deputy Directors
Functional Proponents
SECURITY FUNCTIONAL REQUIREMENTS
Project Officers
TURN OVER
System Managers
ISSE
ISSE
ISSE
Technical Managers
DAA/ISO
ISSO
FSO/ISO
AIS SECURITY REQUIREMENTS SUPPORT
DAA/ISO
ISSO
FSO/ISO
AIS SECURITY REQUIREMENTS SUPPORT

Note: ISSE - Information System Security Engineer(ing)

Source: DFAS Regulation 8000.1-R

Figure 2. Functional Managers' Relationship chart.

The inconsistencies between the organizational alignment in Figure 1 and the functional security alignment in Figure 2 contribute to a breakdown in the security structure itself, as implemented in individual DFAS organizations.

- An Information System Security Engineer is identified in the DFAS Functional Managers' Relationship chart (Figure 2). However, neither the text of the DFAS Regulation nor Figure 1 define the position, its functional responsibilities, or its relationship to the ISSO or other security positions.

[2] The project officer is responsible for AIS security requirements during AIS development and deployment. After the AIS is deployed, the security requirements "turn over" to the System Manager.

- The project officers and system managers are also responsible for AIS security. However, the reporting relationship between those positions and the ISSO is not clearly defined by the DFAS Regulation.

Security Authority, Responsibility, and Access. The DFAS Regulation does not adequately define ISSO responsibilities or give an ISSO the necessary authority to enforce the provisions of the DoD Directive. The DoD Directive assigns specific AIS security responsibilities to the ISSO. Contrary to the DoD Directive, the DFAS Regulation assigns some ISSO responsibilities to other DFAS security positions. For example, the DFAS Regulation deviates from the DoD Directive by assigning the Information Security Officer the responsibility to "ensure that each AIS is operated, maintained, or disposed of in accordance with applicable policies and practices." The DoD Directive assigned this responsibility to the ISSO.

Likewise, DFAS did not provide guidance for ensuring that the ISSO had the authority to enforce security policies on all users with access to the AIS and ensure that users had authorization and a need-to-know. As a result, ISSO responsibilities are changed, and the authority to enforce security policies and safeguards is impaired. For example, the ISSO is supposed to ensure that users of the AIS have proper security clearances and a need-to-know before granting access to the AIS. That requirement is not mentioned as an ISSO responsibility in the DFAS Regulation.

The ISSOs must have the necessary system access to enable them to enforce security policies over all AIS users and to ensure that the users are authorized and have a need-to-know. DFAS did not provide guidance on the access requirements.

- The appointed DCPS ISSO did not have the system access capability necessary to monitor all users to the CP1 and WCC DCPS production platforms. Because user access permissions were not regularly reviewed by the ISSO, more than 3,300 and 800 inactive users were allowed to remain on the DCPS CP1 and WCC platforms, respectively. These users had not accessed the system in more than 90 days, and many had not accessed the system in more than a year. Because inactive user access permissions are more susceptible to compromise, the permissions must be regularly reviewed and removed from the system.[3] The audit did not include a review of unauthorized use of inactive user access permissions. However, those conditions increase the risk of fraud, waste, and abuse. Without required system access, the DCPS ISSO cannot ensure that users have a valid need-to-know, as stipulated by the DoD Directive.

- The primary ISSO for the annuity pay application at the DFAS Denver Center did not have any system access to the application, and the alternate ISSO did not have security administrative capability over

[3] The issue will be addressed in-depth in a later audit report.

any application users. Instead, access capability was granted to individuals assigned to a different operational element within the Directorate of Annuity Pay.

Security Administrative Authority

CA-ACF2 Capabilities. The CA-ACF2 security software used to protect the DCPS production processing environments allows sensitive system administrative privileges to be granted to uniquely identified users. The privileges may be system-wide or restricted in nature.

Security Responsibilities. The DISA Dayton Systems Support Office is responsible for maintaining and controlling the computer mainframe platform, to include the executive software, that supports the DCPS CP1 production environment. The DMC Mechanicsburg has the same responsibilities in support of the DCPS WCC environment. Conversely, DFAS FSA Pensacola is tasked with constructing, operating, and maintaining a computing infrastructure that supports the DCPS application residing on both the CP1 and WCC computer mainframes.

CP1 Production Environment. DFAS FSA Pensacola personnel were granted system-wide sensitive security authority over the DCPS CP1 processing environment, despite the distinct division of responsibilities between the DISA and DFAS organizations. Specifically, four DFAS FSA Pensacola personnel assigned to the Project Support Division were granted system-wide security administrative capability over the CP1 computer mainframe platform. The unrestricted security user privilege allowed updates of the CA-ACF2 databases for administering users and data set access rules. Because DFAS FSA Pensacola originally developed and maintained the DCPS CP1 platform, unrestricted security authority, at that time, was appropriate. However, after DISA assumed responsibility for DCPS mainframe platform support, access granted to the DFAS FSA Pensacola personnel should have been reviewed and limited to DCPS resources. Because DFAS FSA Pensacola access was not restricted, the Dayton Systems Support Office relinquished administrative control of the platform to individuals outside its organization. Consequently, DISA could not ensure that the DCPS production environment was protected from unauthorized access or modification. DISA indicated that it agreed with our audit results and would initiate corrective action to limit the DFAS FSA Pensacola personnel to DCPS resources.

WCC Production Environment. Security administrative authority granted to DFAS FSA Pensacola personnel was adequately restricted to DCPS application resources on the WCC processing platform at the DMC Mechanicsburg.

Summary

To ensure the integrity of application resources and data, DFAS must define, staff, and maintain a security infrastructure that protects the AIS and data from unauthorized modification and destruction. The DoD Directive, in combination with the Security Center Guide, provides instruction for selecting and appointing appropriate personnel to security officer positions within the DoD to ensure one-to-one accountability for each AIS. DFAS should implement the requirements in its security regulation.

DFAS Comments on the Finding and Audit Response

DFAS Comments on the Audit Finding. DFAS provided comments on the audit finding in response to a draft of this report. The following is a summary of issues raised by management, referenced to the related report heading. See Part III for the complete text of management comments.

Adequacy of Security Controls (DCPS ISSO). The DCPS ISSO was placed at a high level to give all aspects of security proper attention and to ensure that corrective actions were taken. Authorized by the DCPS Program Manager, the ISSO has a team that accesses and reports on all aspects of security. On security issues, team members report directly to the ISSO, who also reports on security issues directly to the Program Manager. Although lacking formal security training, the DCPS ISSO is highly qualified for the position and met the other minimum ISSO qualifications cited in the Security Center Guide. Nonetheless, DFAS-wide ISSO qualifications and training requirements do need strengthening.

DoD Directive (Operational Element). DoD Directive 5200.28 states that an ISSO should not report to the operational elements of the AIS over which security requirements must be enforced The DCPS ISSO was positioned within the organization because of the broad responsibilities of an ISSO defined by that directive. On DCPS security matters, the ISSO reports directly to the Program Manager. However, in her position, the ISSO is authorized to enforce security policies worldwide and ensure that users have the required personnel security clearances, authorization, and need-to-know. No other position within the DCPS program satisfies all of these conditions.

DCPS Security (ISSO Training). Knowing where information is and how to obtain it is more critical for an ISSO than being able to personally gather the information. DISA megacenter staff administer and operate the CA-ACF2 security software. The DCPS ISSO responsibilities go far beyond having a technical knowledge of the CA-ACF2 security software because the ISSO deals with all aspects of security worldwide, not just with the systems and people at the FSA. Under the team concept, the DCPS ISSO tasks her team members for CA-ACF2 audit reports (often observing on-line reviews) and other security information on personnel, physical security, and terminal area security. If individuals having CA-ACF2 knowledge were assigned the responsibilities of being the ISSO, those individuals would not have knowledge of the application system.

DCPS Security (System Access Capability). DoD Directive 5200.28 does not specify that an ISSO have system access capability, only that the ISSO "ensure that audit trails are reviewed periodically." To do so, the DCPS ISSO has direct access to any and all CA-ACF2 technicians who have the required system access.

DCPS Security (Direct Line Authority). DoD Directive 5200.28 requires that an ISSO have the authority to enforce security policies and safeguards for all personnel with access to the AIS. However, that requirement does not dictate that the DCPS ISSO have direct line authority over the FSA Pensacola staff performing the day-to-day security functions for the DCPS application. Rather than diminishing, security administration and oversight is enhanced by the current ISSO placement for the DCPS application. The DCPS ISSO is at a high management level and is highly knowledgeable of DCPS. Through her FSA position, the DCPS ISSO has the authority to oversee security related to personnel, facilities, and other aspects Through the DCPS program manager, the DCPS ISSO has worldwide authority for security matters affecting payroll offices and end users.

Security Authority, Responsibility, and Access (Inactive Users). Although there were too many inactive DCPS users, the DCPS ISSO does not need system access to ensure that users have a valid need-to-know. Instead, the ISSO can provide oversight by requesting and acting upon user access reports. Having the DCPS ISSO in an oversight role outside the direct chain of command improves controls since there is no conflict of interest in reporting delays in reducing the number of inactive access.

Audit Response. DFAS comments on the finding were considered in preparing the final report. Although the foregoing information clarified the DFAS position on several issues, we found no reason to change the audit finding and recommendations. The audit response to these comments is provided below and in the Audit Response to management's comments on Recommendations 1.b.(2), 1.b.(3), and 1.b.(4).

Adequacy of Security Controls (DCPS ISSO). The finding addressed the training, authority, and system access of the ISSO appointed for the DCPS application. The report did not dispute the education credentials or qualifications of the DCPS ISSO. Rather, the report emphasized the need for technical CA-ACF2 training for the individual appointed to this ISSO position, and recommended the segregation of the security and systems software maintenance functions.

DoD Directive (Operational Element). The DCPS ISSO cannot accomplish his or her security duties by relying solely on the technical expertise of other staff members, especially when such team members are not under the direct supervision of the ISSO. Without technical knowledge and required system access, the ISSO cannot personally ensure that users have a need-to-know as mandated by DoD Directive 5200.28.

DCPS Security (ISSO Training). Without CA-ACF2 training, the DCPS ISSO cannot be expected to know what kind of security information to request from others or how to interpret such information. This point is illustrated in the example given below.

DCPS Security (System Access Capability). The importance of the DCPS ISSO being able to personally monitor the security environment is best illustrated by an example from the audit. Using CA-ACF2 security software, we identified one DCPS user who had 18 different user IDs. When asked for an explanation, the DCPS ISSO lacked the technical knowledge of the security software and system access needed to identify the user or research the user's access permissions within the CA-ACF2 security database. Once informed of the user's location (payroll office), the DCPS ISSO was able to provide a response by using an employee locator.

DCPS Security (Direct Line Authority). Although theoretically possible, "dotted line" authority over others for security administration or other purposes often proves to be ineffective because a team member's direct line supervisor overrides the indirect authority of others. The DCPS ISSO should have had direct line authority over DFAS Pensacola security staff because they were primarily responsible for the daily DCPS security administration. For example, these security technicians monitored the DCPS security functions and user access permissions, wrote DCPS resource rules, retrieved and reviewed audit reports, and generally responded to all matters related to DCPS application security.

Security Authority, Responsibility, and Access (Inactive Users). As previously stated, absent system access, expertise in using CA-ACF2 software, and direct line authority over DCPS security staff, the DCPS ISSO cannot meet the security requirements under DoD Directive 5200.28. Acknowledged as factual by DFAS, the excessive number of inactive DCPS users identified by the audit does not support management's assertion that DCPS security is improved by the current DCPS security structure.

Recommendations, Management Comments, and Audit Response

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

a. Direct an agency-wide study and take action to:

(1) Appoint qualified personnel to Information System Security Officer positions for each automated information system as mandated by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988.

(2) Incorporate the responsibilities mandated by DoD Directive 5200.28, into position descriptions of all individuals appointed as Information System Security Officers.

Management Comments. DFAS concurred with Recommendations 1.a.(1) and 1.a.(2) to make an Agency-wide study of ISSO positions and revise its security regulation. DFAS agreed to define ISSO responsibilities and minimum qualification standards, including training requirements, in DFAS Regulation 8000.1-R. After the responsibilities and qualification standards are defined, the Director, DFAS, would issue a memorandum requesting assurance from all DFAS Center Directors that all appointed ISSOs are in compliance with the regulation or that required training is scheduled. The director's memorandum would also request that ISSO responsibilities be incorporated into position descriptions.

Audit Response. We consider DFAS comments to Recommendations 1.a.(1) and 1.a.(2) generally responsive, but DFAS did not address ISSOs who are not under the direction and control of center directors, such as the DCPS ISSO, who reports through the Director, DFAS FSO. With its comments on this report, DFAS is requested to provide a copy of the Director's memorandum.

b. Revise the Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," August 21, 1996, to implement the provisions of DoD Directive 5200.28. At a minimum, the regulation should:

(1) Outline specific training requirements for each security position commensurate with assigned functional responsibilities.

(2) Define the operational element of each of the Defense Finance and Accounting Service automated information systems over which security requirements must be enforced.

(3) 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 identified operational elements.

(4) Place the information system security officers in a direct line of authority over personnel performing day-to-day security administration.

Management Comments. DFAS concurred with Recommendation 1.b.(1) and will define the specific training requirements for ISSOs in DFAS Regulation 8000.1-R. DFAS partially concurred with Recommendations 1.b.(2), 1.b.(3), and 1.b.(4). DFAS stated that defining the operational elements of over 180 DFAS systems in DFAS 8000.1-R was unnecessary and impractical because of frequent changes in operating conditions. DFAS further stated that defining the operational element for each system would be arbitrary and inconsistent. Using DCPS as an example, DFAS stated the term "operational element" could encompass maintaining the application software, running programs, processing data, accessing programs, and directing and controlling program management. Because of the size and diversity of DFAS systems, similar definition problems exist for other DFAS systems. These definition problems will continue until all final migratory systems are operational. The organizational security structure defined in DFAS Regulation 8000.1-R supports the principal manager of the system while accommodating the diversity found among DFAS Centers and systems. DFAS stated that implementing Recommendations 1.b.(2), 1.b.(3), and 1.b.(4) to define the operational elements, security chain-of-command, and supervisory lines of authority would seriously impede their ability to appoint the best qualified ISSOs. As an alternative, DFAS agreed to clarify the reporting structure and working relationships among the security officers and the principal manager of the AIS. On all security issues, the ISSO must always be able to openly and directly communicate with the principal AIS manager and the information security managers at DFAS or its centers. The DFAS Regulation 8000.1-R will be revised to include an "ideal" chain-of-command for the ISSO and will recommend that the ISSO not be part of the system end-user population over which the bulk of system access requirements must be enforced.

Audit Response. We disagree with DFAS comments on Recommendations 1.b.(2), 1.b.(3), and 1.b.(4), and therefore, consider the comments nonresponsive. DoD Directive 5200.28 states that an ISSO is to be named for each AIS, and recommends "that the ISSO not report to operational elements of the AIS over which the requirements of this Directive must be enforced." Rather than being unnecessary and impractical, defining the AIS operational elements is key to the overall security administration within any organization, and critical to ensure the independence of the security function, the protection of AIS data and resources, and compliance to the directive. The directive does not distinctly define the term "operational elements," thus allowing each DoD organization the flexibility of defining its own AIS operational elements, as suggested by Recommendation 1.b.(2) Defining the AIS operational elements within DFAS is an important step toward making sure that ISSOs are independent of the operational elements over which they must enforce the security requirements specified by DoD Directive 5200.28.

In its comments, DFAS questioned the practicality of defining the operational element for each AIS because of the large number and diversity of DFAS systems. Instead of defining the unique operational element for each DFAS AIS, the operational elements should be defined in terms of the operational functions that support the AIS. For example, DFAS pointed out that the central design activity at FSA Pensacola could be viewed as an operational element of DCPS. Thus, in concert with Recommendations 1.b.(3) and 1.c., the DFAS security regulation could be revised to specify that ISSOs should not be assigned to operational elements that represent or perform central design activities because of the inherent conflict between the security duties of an ISSO and the software development performed by a central design activity. Had such guidance existed, the DCPS ISSO would not have been established within the central design activity at FSA Pensacola, as is currently the case. Although defining the operational element for diverse AISs might be difficult, common operational functions exist for all AISs. Recognizing these common functions is the first step in identifying the operational elements applicable to all AISs. The complexity of the task should not deter DFAS from complying with the AIS security requirements specified by DoD Directive 5200.28.

The alternative proposed by DFAS of clarifying the reporting structure and working relationships between security managers and principal AIS managers does not meet the intent of Recommendations 1.b.(2), 1.b.(3), and 1.b.(4). Clarifying the reporting structure and working relationships of security personnel in the DFAS regulation will provide a baseline for the overall DFAS security infrastructure. DFAS should emphasize the importance of AIS security by defining the specific reporting structure for ISSOs to ensure that the ISSOs are accountable for and actively involved in the day-to-day security administration. It is also imperative that the ISSOs have the authority necessary to execute the tasks mandated by DoD Directive 5200.28. Such authority cannot be achieved without direct line authority over those responsible for day-to-day security administration.

The diversity of DFAS systems and their operational requirements does present a challenge to DFAS in meeting DoD AIS security requirements. However, the need for strong security controls is the one common factor required for all systems, regardless of size, location, diversity in operations, or management style. In its Report to the Congress, GAO/AIMD-98-127, "Financial Audit: 1997 Consolidated Financial Statements of the United States Government," March 1998, the United States General Accounting Office stated:

> Widespread computer control weaknesses are placing enormous amounts of federal assets at risk of fraud and misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. Significant information security weaknesses in systems that handle the government's unclassified information have been reported in each of the major federal agencies. The most serious reported problem is inadequately restricted access to sensitive data. In today's highly computerized and interconnected environment, such weaknesses are vulnerable to exploitation by outside intruders as well as authorized users with malicious intent.

By implementing the recommendations made in this report, DFAS has the opportunity to demonstrate its commitment toward strengthening AIS security over all DFAS applications and providing a baseline for building a solid security structure.

We request that DFAS reconsider its position on Recommendations 1.b.(2), 1.b.(3), and 1.b.(4) in its response to this final report.

c. Revise the Defense Finance and Accounting Service Regulation 8000.1-R to include specific segregation of duties among application support functions, e.g., security and software development.

Management Comments. DFAS concurred with Recommendation 1.c., stating that DFAS 8000.1-R would be revised to incorporate the required changes.

d. Require each Designated Approving Authority to perform and report on annual security compliance reviews to ensure that qualified information system security officers are appointed for each automated information system and that the officers have the training and system access necessary to perform their duties.

Management Comments. DFAS concurred with Recommendation 1.d. and stated that DFAS 8000.1-R would be revised to incorporate the required changes.

2. We recommend that the Chief, Systems Support Office, Defense Information Systems Agency, Defense Megacenter, Mechanicsburg, Pennsylvania, review the sensitive security administrative authority on the Defense Civilian Pay System CP1 production platform and limit access of the Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, personnel to Defense Civilian Pay System application resources.

Management Comments. DISA concurred with the recommendation. The CP1 system was migrated to DMC Mechanicsburg in July 1998 and consolidated with the Pensacola (WCC) image in November 1998. After consolidation, DMC Mechanicsburg was to review and restrict sensitive administrative authority to authorized personnel.

Other Management Comments. In unsolicited comments, DFAS stated that access had been limited in accordance with Recommendation 2.

Audit Response. Contrary to management's assertion, at the date DFAS provided its comments, DFAS FSA Pensacola personnel had not been limited to civilian pay resources on the CP1 production platform.

Part II - Additional Information

Appendix A. Audit Process

Scope

Work Performed. We examined security controls over the DCPS production processing environments resident on mainframe computers located at the DISA Defense megacenters in Mechanicsburg and Denver. The DCPS application currently services approximately 700,000 employees and processes more than $35 billion in payroll transactions. To test security rules and features and access authorizations, we used the audit features of the CA-ACF2 security software. We discussed the tests and verified the results with DFAS FSA Pensacola personnel. The test results were reported in Part I of this report. We also used the CA-CULPRIT report writer to exact security authorization data directly from the CP1 and WCC DCPS platform security databases.

While identifying security issues pertinent to the DCPS application, we noted a pattern of noncompliance to the DoD Directive. As a result, audit evaluation specific to the DCPS application was delayed to further research and report on the DFAS security problems discussed in Part I of this report. Audit work on security controls over the DCPS application will continue under Inspector General, DoD, Project No. 7FD-2023.01.

To determine the root cause for continued security problems within DFAS, we evaluated DFAS implementation of the DoD Directive as outlined in the DFAS Regulation. Specifically, we evaluated DFAS direction for:

- the assignment of ISSOs and security responsibilities,
- the reporting structure for ISSOs within the DFAS organization structure, and
- specific qualifications and training requirements for individuals appointed to ISSO positions.

In addition, we interviewed security personnel at DFAS and its Cleveland and Denver Centers to determine their interpretation and implementation of the regulation at their specific sites. We also included limited audit evaluation of security controls over the DFAS Defense Retiree and Annuitant Pay System at the DFAS Denver Center.

Limitations to Audit Scope. Because of the size and complexity of DCPS, we limited our review to security controls over the DCPS application as discussed above. Thus, we did not evaluate the DCPS security controls on a separate National Security Agency platform. The audit did not include a review to determine whether DCPS data had been accessed or modified without proper authorization. Therefore, we detected no instances of fraud, waste, or abuse. A review of the management control program will be accomplished in a subsequent audit report on DCPS security.

DoD-wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting these objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Fundamentally reengineer the Department and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

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 objective and goal.

- **Objective:** Ensure that DoD vital information resources are secure and protected. **Goal:** Assess 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 Management and Technology high risk area.

Methodology

Use of Computer-Processed Data. We relied on computer-processed data extracted from the security software database provided by CA-ACF2 for the CP1 and WCC platforms. All system testing and use of security software audit tools were accomplished in a controlled environment with management's approval. We used automated and manual techniques to analyze system data. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Audit Type, Dates, and Standards. This financial-related audit was performed from May 1997 through April 1998. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

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

Summary of Prior Coverage

During the last 5 years, the Inspector General, DoD, issued one report that has direct correlation to the DFAS security issues discussed in Part I of this report. Specifically, Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996, addresses DFAS noncompliance with the DoD Directive. The audit focused on application and security software controls safeguarding the data integrity of the Defense Joint Military Pay System. In addition to security software problems, the report recommended that the Director of Military Pay, DFAS Indianapolis, Indiana, establish an ISSO position within the Directorate of Military Pay. It was further recommended that the ISSO report directly to the Director of Military Pay and that the ISSO be responsible for monitoring system access for all users. DFAS Indianapolis concurred. An ISSO position was created with direct reporting to the Chief, Business Management Office, in the Directorate of Military Pay.

The report also recommended that the Director of Military Pay, DFAS Denver Center realign the directorate so the ISSO would have direct reporting to the Director of Military Pay. DFAS agreed to redefine the roles and relationships of the Defense Joint Military Pay System ISSOs by way of a Memorandum of Agreement. Accordingly, the Project Officer for this application will ensure that the ISSOs and the Directors of Military Pay enforce security for the payroll application at all affected DFAS centers.

Appendix B. 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 Information Systems Agency
  Defense Wide Information Assurance Program
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

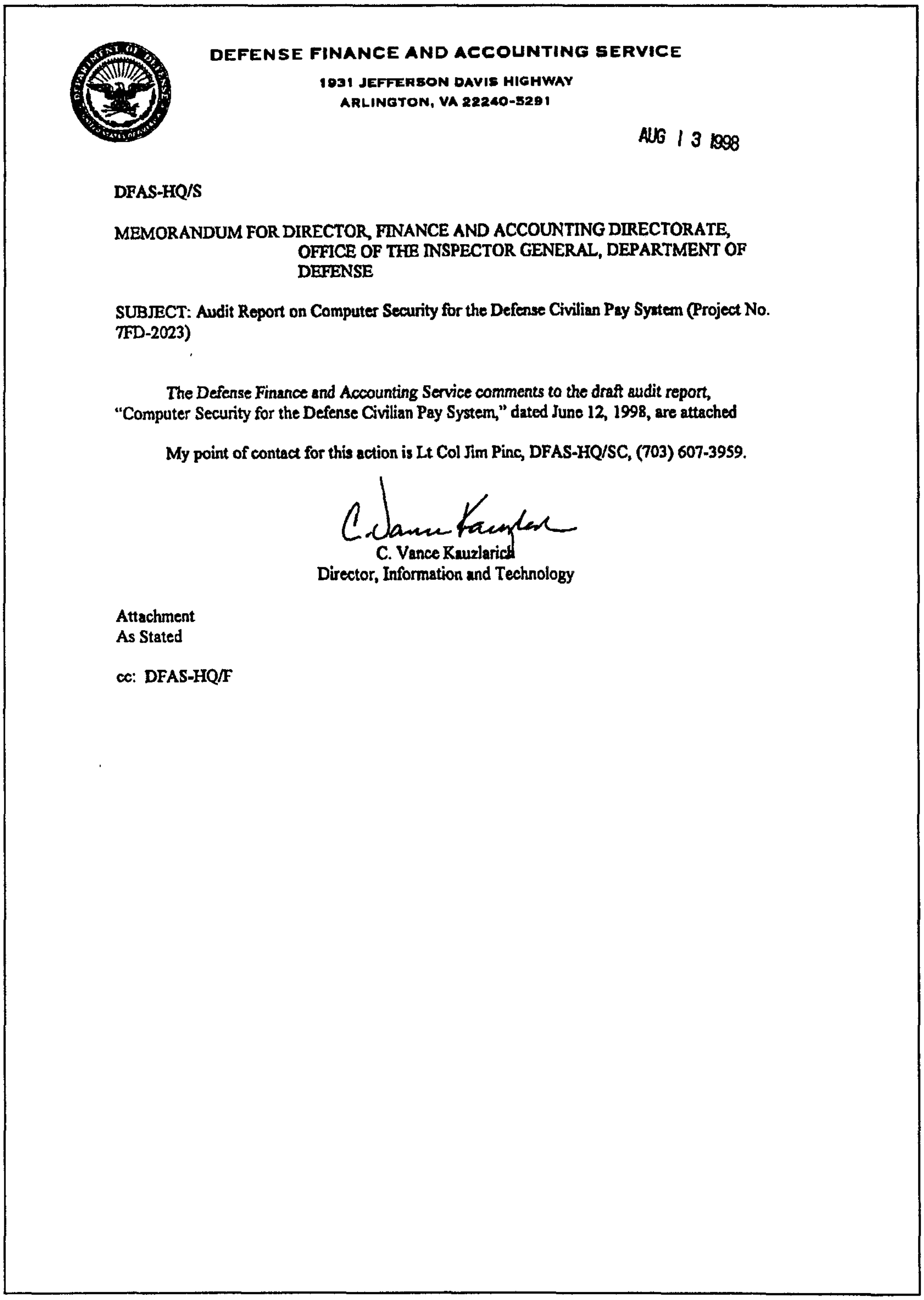
Office of Management and Budget
Technical Information Center, National Security and International Affairs Division,
General Accounting Office

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 Defense, Committee on Appropriations
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs and International Relations, Committee on Government Reform
House Committee on Armed Services

Part III - Management Comments

Defense Finance and Accounting Service Comments



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

AUG 13 1998

DFAS-HQ/S

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

SUBJECT: Audit Report on Computer Security for the Defense Civilian Pay System (Project No. 7FD-2023)

The Defense Finance and Accounting Service comments to the draft audit report, "Computer Security for the Defense Civilian Pay System," dated June 12, 1998, are attached

My point of contact for this action is Lt Col Jim Pinc, DFAS-HQ/SC, (703) 607-3959.

C. Vance Kauzlarich
Director, Information and Technology

Attachment
As Stated

cc: DFAS-HQ/F

DFAS COMMENTS ON FINDINGS AND RECOMMENDATIONS TO DODIG DRAFT REPORT (PROJECT NO. 7FD-2023)

Part I - Audit Results

Adequacy of Security Controls

DoDIG Comment, page 4:

DFAS FSA Pensacola designated an individual as the DCPS Information System Security Officer (ISSO) when the person did not have the training, authority, or system access necessary to adequately enforce security policies and safeguards on all personnel with access to the application.

DFAS Comments:

Within the DCPS Program, it was a conscious decision to place the ISSO at a high enough level that all aspects of security could receive proper attention and could initiate and ensure corrective action is taken when required. The ISSO position is the Director, Software Engineering Division of the Civilian Pay Systems Engineering Directorate within FSA-PE. The incumbent of this position has proper authority since she has been designated as the ISSO by the DCPS Program Manager in accordance with DFAS Regulation 8000.1-R. Under this authority, she has gathered a team that accesses and reports on security matters not only concerning the system, but also data communications, personnel, facilities, and end users requirements. Team members report directly to the ISSO regarding security matters and the ISSO reports directly to the Program Manager. We acknowledge that the incumbent has received no formal Security training.

On page 8 of the report, you suggest that the "ISSO possess a technical degree in computer science, mathematics, electrical engineering, or a related field. The minimum ISSO qualifications recommended by the Security Center Guide are:

- 2 years' experience in a computer-related field,
- 1 year of computer security experience or mandatory computer security training, and
- familiarization with the AIS operating system.

The current DCPS ISSO has been employed in the computer science field for 14 years. She has a Computer Science Degree and additional course work which, when added to her Computer Degree, equate to an Electrical Engineering Degree. She has a minor in Calculus and the majority of her work toward a Masters Degree in Mathematics has been in Vector Analysis and Statistics. Her position as Director of the Software Engineering Division ensures she is very familiar with the operating system. Since the start of this audit, she has become very knowledgeable of all security requirements and reporting procedures, and we believe she is highly qualified to be the ISSO for DCPS.

Nonetheless, DFAS concurs with your general findings that ISSO qualification and training requirements need strengthening DFAS-wide. Your recommendations for corrective actions regarding ISSO qualifications, responsibilities, and training, with which we concur, should remedy this situation.

DoDIG Comment, page 4:

DFAS did not uniformly implement security on other key financial applications throughout the organization.

DFAS Comment:

Please see DFAS comments for Recommendation 1.b.

Security Guidance

DoDIG Comment, page 5:

The ISSO should not report to operational elements of the AIS over which security requirements must be enforced. The ISSO will have security responsibility and authority for the AIS. Specifically, each ISSO must:

- ensure that the AIS is maintained and disposed of in accordance with internal security policies and practices;
- have the authority to enforce security policies and safeguards on all users who have access to the AIS for which the ISSO is responsible; and
- ensure that users have the required personnel security clearances, authorization, and need-to-know.

DFAS Comment:

The responsibilities for the ISSO are very broad and the reason that the DCPS ISSO is in the position designated. In security matters, the ISSO reports directly to the Program Manager. In addition, in her position, she can ensure the AIS is maintained in accordance with internal security policies, she has the authority to enforce security policy worldwide, and she can ensure that users have the required personnel security clearances, authorization, and need-to-know. There is no other position within the DCPS program

program that satisfies all these conditions. Please also see DFAS comments for Recommendation 1b.

DCPS Security

DODIG Comment, page 6:

The ISSO was not trained on the technical aspects of CA-ACF2, the external security software used to protect the DCPS application. As a result, the ISSO did not possess the specific technical knowledge and skills necessary to adequately review audit files and user access permissions

DFAS Comment:

The CA-ACF2 software is administered and operated by DISA Megacenter personnel. The DCPS ISSO tasks her team members to provide audit reports, and often sits with the person during on-line reviews. This method of accomplishing ISSO duties is consistent with the concept of using the personnel staffing specialist "team member" for personnel security issues, the facilities security manager "team member" for issues of physical security, and the Terminal Area Security Officer "team member" for terminal area security. The responsibilities of the ISSO go far beyond CA-ACF2 technical knowledge. The DCPS ISSO must deal with all aspects of security, not just systems and with people not only at the FSA, but at the MegaCenters, payroll offices, and activities throughout the world. We feel it is more critical that the ISSO understands where information is and how to obtain information rather than the requirement to gather all information herself. If the individuals having CA-ACF2 knowledge were assigned the responsibility of being the ISSO, those individuals would not have knowledge of the application system.

DODIG Comment, page 6:

The ISSO did not have the system access capability necessary to monitor or administer security control over all users to the CP1 and WCC DCPS production platforms as mandated by the DoD Directive.

DFAS Comment:

DoDD 5200.28 requires that the ISSO "Ensure that audit trails are reviewed periodically." It does not specify that the ISSO have system access capability in order to ensure this function is performed. Although it is certainly true that a CA-ACF2 technician is required to perform systems monitoring functions, we believe it more appropriate to not designate this individual as the ISSO, recognizing that the responsibilities of the ISSO go well beyond those of any technician. In the capacity as ISSO, the incumbent has direct access to any/all technicians necessary for performance of this aspect of ISSO responsibilities.

DODIG Comment, page 6:

The ISSO did not have direct line of authority over the DFAS FSA Pensacola staff performing the day-to-day security functions for the DCPS application. Thus, the authority and control of the ISSO over the daily accomplishment of security administration and oversight were diminished. Specifically, the appointed ISSO was the Chief of the Software Engineering Division.

DFAS Comment:

In our assessment, a requirement does not exist for the ISSO to have direct line authority over the DFAS FSA-Pensacola staff performing the day-to-day security functions for the DCPS application. The DoDD 5200.28 requirement of the ISSO having "the authority to enforce security policies and safeguards on all personnel having access to the AIS" does not necessarily translate to a requirement for direct line authority. In the case of DCPS, we not only non-concur with the assertion that our current ISSO placement diminishes the security administration and oversight, we believe the placement of the ISSO actually increases administration and oversight. The DCPS ISSO:

- Is at a high management level ensuring security is given proper attention.
- Is in a position that is highly knowledgeable of the DCPS AIS.
- Has the authority, through her position in the FSA, to provide oversight for security involving personnel, facilities, communication, etc.
- Has the authority, through the DCPS Program Manager, for security matters affecting the payroll offices and end users throughout the world.

DFAS Security Implementation

DoDIG Comment, page 7:

The DFAS Regulation did not provide adequate guidance to achieve uniform implementation of security policy throughout DFAS and did not ensure appropriate assignment of security responsibilities.

DFAS Comment:

DFAS concurs with the general findings that ISSO appointment procedures, training requirements, and a more clear understanding of responsibilities would be beneficial, as discussed under Recommendations for Corrective Actions below.

DODIG Comment, page 9:

The DFAS Regulation "does not define the specific chain-of-command for the ISSO position or placement of the position in the DFAS organization structure. Following the lead of other organizations within the DoD, DFAS must ensure that the security function is placed within the organization structure to provide the independence and authority necessary to protect the application data."

DFAS Comment:

Please see DFAS comments for Recommendation 1.b.

DoDIG Comments, page 10-12:

The report notes some undefined and inconsistent areas when considering the security organizational structure as defined in DFAS Regulation 8000.1-R.

DFAS Comment:

DFAS generally concurs with these findings, and will take action as discussed under Recommendations for Corrective Actions below.

DODIG Comment, page 13:

The appointed DCPS ISSO did not have the system access capability necessary to monitor all users to the CP1 and WCC DCPS production platforms. Because user access permissions were not regularly reviewed by the ISSO, more than 3,300 and 800 inactive users were allowed to remain on the DCPS CP1 and WCC platforms, respectively. These users had not accessed the system in more than 90 days, and many had not accessed the system in more than a year. Because inactive user access permissions are more susceptible to compromise, the permissions must be regularly reviewed and removed from the system.[1] The audit did not include a review of unauthorized use of inactive user access permissions. However, those conditions increase the risk of fraud, waste, and abuse. Without required system access, the DCPS ISSO cannot ensure that users have a valid need-to-know, as stipulated by the DoD Directive.

DFAS Comment:

DFAS acknowledges that there are too many inactive users in the DCPS databases. We will take action to eliminate the inactive access and monitor this area in the future. However, it does not necessarily follow that the ISSO must have system access to ensure that users have a valid need-to-know. The ISSO provides oversight of the security process and can request reports showing statistics on user access and take appropriate action as necessary. In this

[1] The issue will be addressed in-depth in a later audit report.

instance, there is improved control since the person performing the oversight responsibility is not in the direct chain of command in which there may be a conflict of interest in reporting delays in reducing the number of inactive access.

Security Administrative Control

DODIG Comment, page 14:

DFAS FSA Pensacola personnel were granted system-wide sensitive security authority over the DCPS CP1 processing environment, despite the distinct division of responsibilities between the DISA and DFAS organizations. Specifically, four DFAS FSA Pensacola personnel assigned to the Project Support Division were granted system-wide security administrative capability over the CP1 computer mainframe platform. The unrestricted security user privilege allowed updates of the CA-ACF2 databases for administering users and data set access rules. Because DFAS FSA Pensacola originally developed and maintained the DCPS CP1 platform, unrestricted security authority, at that time, was appropriate. However, after DISA assumed responsibility for DCPS mainframe platform support, access granted to the DFAS FSA Pensacola personnel should have been reviewed and limited to DCPS resources. Because DFAS FSA Pensacola access was not restricted, the Dayton Systems Support Office relinquished administrative control of the platform to individuals outside its organization. Consequently, DISA could not ensure that the DCPS production environment was protected from unauthorized access or modification. DISA agreed with our evaluation and initiated corrective action to limit the DFAS FSA Pensacola personnel to DCPS resources.

DFAS Comment:

DFAS concurs with the finding. Although DISA has been requested on more than one occasion to remove the access for FSAPE personnel, it has not yet been accomplished. .

DODIG Recommendations for Corrective Action

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

a. Direct an agency-wide study and take action to:

1. Appoint qualified personnel to Information System Security Officer positions for each automated information system as mandated by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988.

2. Incorporate the responsibilities mandated by DoD Directive 5200.28, into position descriptions of all individuals appointed as Information System Security Officers.

DFAS Comment to 1.a.:

DFAS concurs. DFAS-HQ/S will take action to define responsibilities and minimum qualification standards, including training requirements, for Information System Security Officers (ISSOs), and incorporate them into the current DFAS Regulation 8000.1-R, "Information Management Policy and Instructional Guidance." Estimated completion date is September 30, 1998. At that time, DFAS-HQ/S will prepare a memorandum for distribution to all DFAS Center Directors under the signature of the DFAS Director requesting assurance that all appointed ISSOs are in compliance, or that required training is scheduled. Incorporation of ISSO responsibilities into position descriptions also will be requested. Estimated completion date for distributing the memorandum is October 30, 1998.

b. Revise the Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," August 21, 1996, to implement the provisions of DoD Directive 5200.28. At a minimum, the regulation should:

1. Outline specific training requirements for each security position commensurate with assigned functional responsibilities.

2. Define the operational element of each of the Defense Finance and Accounting Service automated information systems over which security requirements must be enforced.

3. 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 identified operational elements.

4. Place the information system security officers in a direct line of authority over personnel performing day-to-day security administration.

DFAS Comment to 1.b.:

As noted for Recommendation 1.a., DFAS concurs with specifying training requirements for ISSOs, and will take action as described above. DFAS, however, can only partially concur with Recommendations b.2., b.3, and b.4. First, DFAS currently has over 180 automated information systems for which defining in DFAS Regulation 8000.1-R the operational element of each system is unnecessary and impractical. For example, a regulation contains policy. The certification and accreditation of systems requires input from the various components that support a system internal and external to DFAS. These components change with some frequency and should not be in a policy document. If the users are considered operational elements and since DFAS operates DoD wide systems, it is impractical to list, in a regulation, all Navy, Air Force, etc. local area networks over which security must be enforced. Second, defining the operational element for each system would be arbitrary and inconsistent. In the case of DCPS, for example, does the central design activity (Pensacola FSA) which maintains the application software become the operational

element, or the Defense Megacenter where the program is run and the data processed? Or payroll office users who access the program, or the program manager's staff which directs and controls many aspects of civilian payroll processing? The entire process is an operational process and any of the above elements could be defined as an operational element. Similar definition problems exist for all other DFAS systems--systems that are widely diverse. DFAS has small systems and large ones, systems managed within one Center and across multiple Centers, central design activities within DFAS and outside of DFAS, full-time ISSOs and part-time ISSOs, and varying management cultures inherited from the Military Services. Until all final migratory systems are fully operational, DFAS necessarily must contend with this operational variability. As such, the DFAS organizational security structure defined in DFAS Regulation 8000.1-R is intended to support the principal manager of the system (the Program Manager, Project Officer, or System Manager), who is charged with primary security responsibilities for his or her system, while accommodating the diversity found among Centers and systems. DFAS has discussed these recommendations, including with all Information Security Managers (one assigned to each Center) in a DFAS AIS security conference in July 1998, and DFAS remains unconvinced that acting on Recommendations b.2, b.3, and b.4, as stated, would be beneficial. Mandating a specific chain-of-command and reporting structure uniformly for all ISSOs throughout DFAS, while ensuring they do not report to an operational element and yet have direct line of authority over personnel performing day-to-day security administration, would seriously impede our ability to appoint the best qualified ISSOs. Such restrictions would be counterproductive in allowing our Program Managers/Project Officers/System Managers and their ISSOs to fully discharge their duties and responsibilities

As alternative corrective actions, we agree that the reporting structure and working relationships, including lines of responsibility and the flow of information, among the ISSO, the principal manager of the system, and other security officials should and can be clarified in DFAS Regulation 8000.1-R. In all cases, the ISSO must be able to openly and directly communicate any system security incidents or issues to the principal manager of the system and to the Information Security Manager at his or her Center, or DFAS-HQ in the case of FSAPE and FSAPR. Changes to the regulation also should include a recommended "ideal" chain-of-command for the ISSO and the recommendation that the ISSO not be part of the system end-user population over which the bulk of system access requirements must be enforced. Estimated completion date for these alternative actions is September 30, 1998.

c. Revise the Defense Finance and Accounting Service Regulation 8000.1-R to include specific segregation of duties among application support functions, e.g. security and software development.

DFAS Comment to 1.c.:

DFAS concurs. DFAS will clarify segregation of security and software development duties as part of the DFAS Regulation 8000.1-R revisions to be made by September 30, 1998.

d. Require each Designated Approving Authority to perform and report on annual security compliance reviews to ensure that qualified information system security officers are appointed for each automated information system and that the officers have the training and system access necessary to perform their duties.

DFAS Comment to 1.d.:

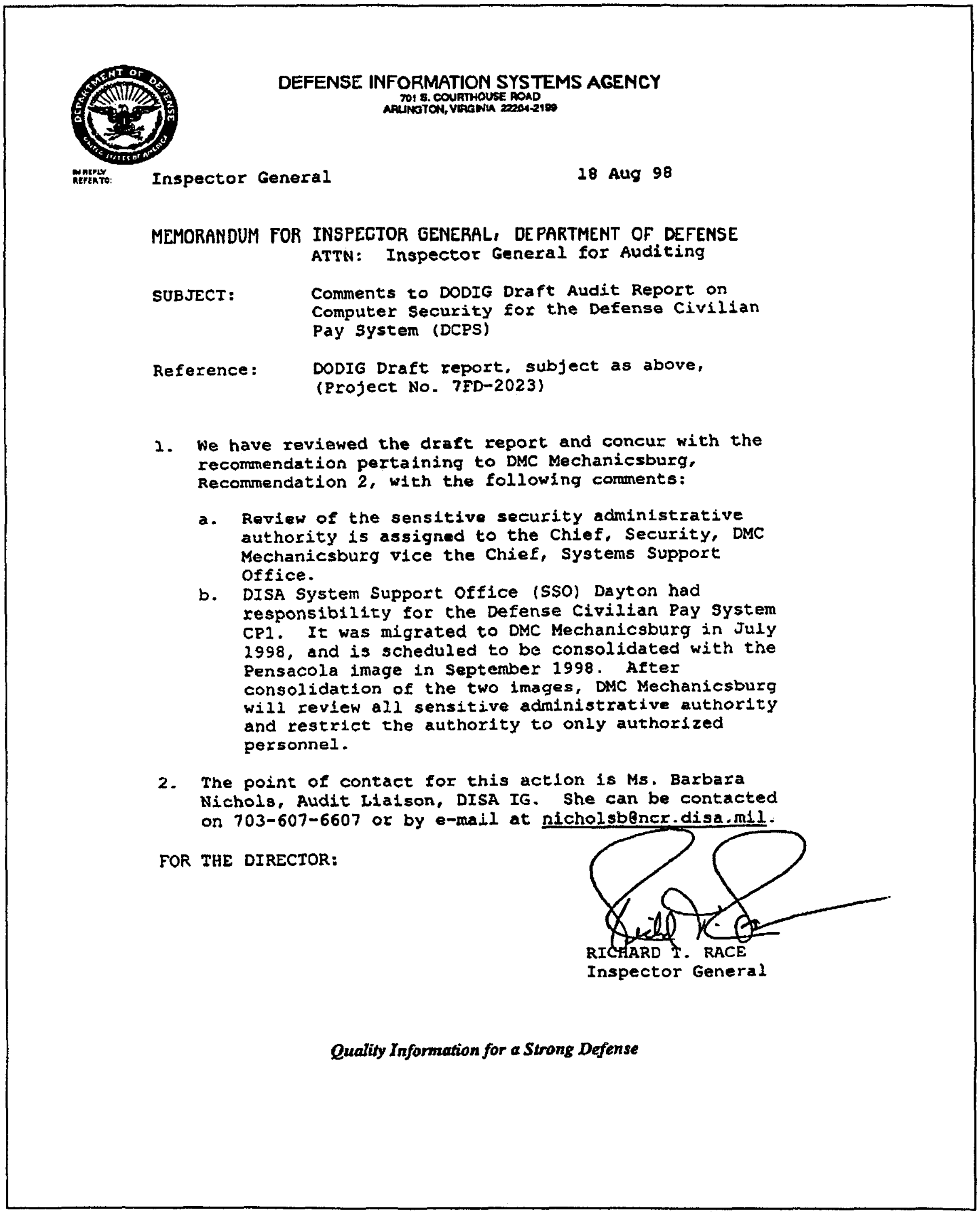
DFAS concurs. DFAS intends to make this requirement integral to the post-accreditation phase of our certification and accreditation risk-based management process, in which annual reviews are a current requirement. To carry out this corrective action, DFAS will incorporate it into the DFAS Regulation 8000.1-R revisions to be made by September 30, 1998, and incorporate the same provisions into its Performance Assessment Internal Control function.

2. We recommend that the Chief, Systems Support Office, Defense Information Systems Agency, Defense Megacenter, Mechanicsburg, Pennsylvania, review the sensitive security administrative authority on the Defense Civilian Pay System CP1 production platform and limit access of the Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, personnel to Defense Civilian Pay System application resources.

DFAS Comment to 2.:

DFAS concurs. Access has been limited in accordance with this recommendation.

Defense Information Systems Agency Comments



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

IN REPLY REFER TO: Inspector General 18 Aug 98

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Inspector General for Auditing

SUBJECT: Comments to DODIG Draft Audit Report on Computer Security for the Defense Civilian Pay System (DCPS)

Reference: DODIG Draft report, subject as above, (Project No. 7FD-2023)

1. We have reviewed the draft report and concur with the recommendation pertaining to DMC Mechanicsburg, Recommendation 2, with the following comments:

   a. Review of the sensitive security administrative authority is assigned to the Chief, Security, DMC Mechanicsburg vice the Chief, Systems Support Office.

   b. DISA System Support Office (SSO) Dayton had responsibility for the Defense Civilian Pay System CP1. It was migrated to DMC Mechanicsburg in July 1998, and is scheduled to be consolidated with the Pensacola image in September 1998. After consolidation of the two images, DMC Mechanicsburg will review all sensitive administrative authority and restrict the authority to only authorized personnel.

2. The point of contact for this action is Ms. Barbara Nichols, Audit Liaison, DISA IG. She can be contacted on 703-607-6607 or by e-mail at nicholsb@ncr.disa.mil.

FOR THE DIRECTOR:

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

Audit Team Members

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

F. Jay Lane
Brian M. Flynn
W. Andy Cooley
Frances E. Cain
Ben J. Meade
Debra L. Sherwood