Audit Report

INFORMATION ASSURANCE OF THE DEFENSE CIVILIAN PERSONNEL DATA SERVICE

Report No. 98-082 February 23, 1998

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Information Assurance of the Defense Civilian Personnel Data Service

B. DATE Report Downloaded From the Internet: 09/23/99

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

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/23/99**

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

Additional Information and 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.OSDMIL.

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

CPMS	Civilian Personnel Management Service
DAA	Designated Approving Authority
DCPDS	Defense Civilian Personnel Data System
DITSCAP	DoD Information Technology Security Certification and Accreditation Process

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

February 23, 1998

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, CIVILIAN PERSONNEL MANAGEMENT SERVICE

SUBJECT: Audit Report on Information Assurance of the Defense Civilian Personnel Data System (Report No. 98-082)

We are providing this audit report for review and comment. This is the second of four reports on the Defense Civilian Personnel Data System by the Office of the Inspector General, DoD. In addition, the Army Audit Agency and the Air Force Audit Agency will issue separate reports on the Army and Air Force Information Assurance in the Defense Civilian Personnel Data System, respectively. We considered management comments on a draft of this report in preparing the final report.

Comments from the Air Force were responsive. Comments from the Civilian Personnel Management Service were partially responsive. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not provide comments on the draft of this report. DoD Directive 7650.3 requires that all recommendations be resolved promptly. Therefore, we request the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to comment on Recommendation 1. and the Director, Civilian Personnel Management Service, to provide comments on Recommendation 2. and milestones for the agreed-upon risk assessment action plan by March 23, 1998.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone, Audit Program Director, at (703) 604-9049 (DSN 664-9049); Ms. Cecelia A. Miggins, Audit Project Manager, at (703) 604-9046 (DSN 664-9046); or Mr. Karim Malek, Audit Team Leader, at (703) 604-9039 (DSN 664-9039). See Appendix F for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman

Robert-J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-082
(Project No. 7RE-3006.01)

February 23, 1998

Information Assurance of the Defense Civilian Personnel Data System

Executive Summary

Introduction. The Defense Civilian Personnel Data System (DCPDS) is an automated information system that will process sensitive-but-unclassified personnel information for at least 750,000 DoD civilian records at 23 regional personnel servicing centers and approximately 300 customer support units. The Air Force Personnel Center is developing DCPDS and reports DCPDS progress to the Major Automated Information Systems Review Council through the Office of the Assistant Secretary of the Air Force (Acquisition) and the Commander, Electronics Systems Center, Air Force Materiel Command. DCPDS life-cycle program costs are estimated at $795 million. DCPDS is scheduled for initial operational capability in June 1998 and full operational capability in September 1999.

Audit Objectives. The overall audit objective was to determine the adequacy of the information assurance program for major automated information systems. Specifically, for this audit, we evaluated DCPDS security planning, risk analysis, and security management. We also evaluated the DCPDS management control program as it related to the audit objectives.

Audit Results. The Director, Information Assurance, Office of the Assistant Secretary Defense (Command, Control, Communications, and Intelligence), in coordination with the functional program manager and the acquisition program manager, initiated actions to determine DCPDS information assurance solutions. However, without aggressive management action, the DCPDS information assurance program will not have adequate controls in place to safeguard DCPDS data and computer resources for the target system when that system is implemented at selected sites, which is currently planned for June 1998. As a result, DCPDS has high risks of unauthorized system access; intentional or unintentional alteration and destruction of personnel data; and denial of service to authorized users. See Part I for the complete discussion and Appendix A for details on the management control program.

Summary of Recommendations. We recommend strengthened oversight and management of DCPDS information assurance. We also recommend the establishment of information assurance functional requirements and the implementation of information assurance measures to protect DoD civilian personnel data.

Management Comments. The Air Force generally concurred with the finding and recommendations. The Director, Civilian Personnel Management Service, generally agreed with the finding, but nonconcurred with two of three recommendations. The Director stated that, by acquiring C-2 compliant system hardware and software, there

would be no perceivable threats in the DCPDS processing environment that must be countered by system design. In addition, the Director stated that a computer security response team, representing the Major Automated Information Systems Review Council, identified risks to DCPDS through a facilitated risk assessment program, and the acquisition program manager is developing an action plan to mitigate program risks. The Director nonconcurred with a draft recommendation to revise the operational requirements document to include validated threat information and also nonconcurred with the recommendation to provide the acquisition program manager with functional threat requirements and funding to protect the DoD civilian personnel data. The Director stated that the facilitated risk analysis provided a comprehensive list of threats and is a more appropriate analysis for the DCPDS. The Director also stated that he does not recognize coordination with the acquisition program manager as a problem and that there are no funding deficiencies for protecting DoD civilian personnel data. The Director agreed with the recommendation to coordinate and approve a certification and accreditation plan to protect the DCPDS and commented that his office is determining which organizational component will serve as the operating DCPDS designated approving authority. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), did not comment on a draft of this report issued October 3 1, 1997. See Part I for a discussion of management comments and Part III for the complete text of the management comments.

Audit Response. The Air Force comments were responsive. The Director, Civilian Personnel Management Service, comments were only partially responsive. As a result of the Director's comments, we deleted the draft recommendation to revise the operational requirements document and revised the recommendation to provide the acquisition program manager with functional security requirements and funding to protect the DoD civilian personnel data. We disagree with the Director's assessment of the level of assurance provided by acquiring C-2 compliant system hardware and software. We request that the Director, Civilian Personnel Management Service, provide comments on the final report as indicated in Part I. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), provide comments on the final report by March 23, 1998.

Table of Contents

Part I - Audit Results

Audit Background

This report discusses our audit of the Defense Civilian Personnel Data System (DCPDS) information assurance program. The DCPDS will provide a seamless automated information system for civilian personnel policy actions and personnel decisions during peacetime, contingencies, and wartime. The DCPDS will support DoD Components worldwide and will be used by personnel officials, employees, managers, and senior leadership at all levels of DoD operations. DCPDS will store, process, and transmit data for 750,000 personnel records that are subject to the Privacy Act of 1974 and the Freedom of Information Act. For security purposes, the DCPDS data are labeled "sensitive-but-unclassified. "

Defense Civilian Personnel Data System. The DCPDS will enable the DoD Components to process, store, and transmit civilian personnel records on data bases at 23 regional personnel servicing centers and approximately 300 base-level personnel units. Information in the regional data bases will be periodically replicated to a single DoD corporate data base to generate reports for DoD managers. The Office of the Civilian Personnel Management Service assigned the DCPDS acquisition program manager, the Technical Director, Directorate of Personnel Data Systems, Air Force Personnel Center, responsibility for the overall protection of the DCPDS information and the computer resources.

The DCPDS program is a major automated information system and is classified as Acquisition Category IAM. The program is subject to the provisions of DoD Directive 5000.1, "Defense Acquisition," March 15, 1996, and DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, " March 15, 1996. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), as the DoD Chief Information Officer, is the DCPDS milestone decision authority and approves program entry into new life-cycle phases.

The Civilian Personnel Management Service, through the Deputy Assistant Secretary of Defense (Civilian Personnel Policy), is the functional proponent of DCPDS, and the Office of the Assistant Secretary of the Air Force (Acquisition) is the Executive Agent for the DCPDS acquisition. The Commander, Electronics Systems Center, Air Force Materiel Command, is the DCPDS designated acquisition commander, and the Air Force Personnel Center staffs the DCPDS development organization. Although a complete program cost estimate is not available, the Civilian Personnel Management Service estimated in a September 29, 1997, Economic Analysis, DCPDS investment costs to be about $350 million and program life-cycle costs to be about $795 million. The Civilian Personnel Management Service also estimated total human resources mission area costs including the DCPDS life-cycle program

costs to be about $10.3 billion, with total program benefits of $2.3 billion. Additionally, the Air Force Cost Analysis Agency is performing a sufficiency review of the DCPDS software development costs. The DCPDS initial operational capability is scheduled for June 1998, and full operational capability is scheduled for September 1999.

Safeguarding Personnel Data. DoD civilian personnel data are subject to provisions of the Privacy Act of 1974 and the Freedom of Information Act. The Privacy Act generally requires Federal agencies to safeguard personal information from disclosure to any other organization or individual without the consent of the individual to whom the information pertains. The Privacy Act also requires each agency to account for disclosures of information to other organizations and individuals. The Freedom of Information Act requires agencies to make information available to the public but excludes from that disclosure personnel information that would constitute an invasion of privacy. The DCPDS must meet provisions of the Computer Security Act of 1987 to safeguard the personnel data.

The policy and procedures for safeguarding sensitive-but-unclassified DoD information are prescribed in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988. "Information assurance" and "computer security," as used in this report, are intended to be synonymous and refer to the process used to protect and defend information and information systems by ensuring their confidentiality, integrity, availability, and non-repudiation. Information assurance includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. Please see Appendix D for a glossary of additional terms used in this report.

Audit Objectives

The overall audit objective was to determine the adequacy of the information assurance program for major automated information systems. Specifically, for this audit, we evaluated DCPDS security planning, risk analysis, and security management. We also evaluated the DCPDS management control program as it relates to the audit objectives (Appendix A). See Appendix B for a discussion of prior audit coverage and Appendix C for other matters of interest regarding the interim certification for the Air Force civilian personnel system.

Information Assurance for the DoD Civilian Personnel Data System

The Director, Information Assurance, Office of the Assistant Secretary Defense (Command, Control, Communications, and Intelligence), in coordination with the functional program manager and the acquisition program manager, initiated actions to determine DCPDS information assurance solutions. However, the target DCPDS will not have controls in place to adequately safeguard 750,000 civilian personnel records and the computer resources used to process those records. Controls include computer security measures to protect the system's data and resources and to provide the confidentiality, integrity, and availability of the system for individuals authorized to use it.

The controls are lacking because the DCPDS functional and acquisition program managers did not sufficiently recognize or define information assurance requirements. Specifically, the functional and acquisition program managers:

o did not adequately recognize or define system threats during DCPDS requirements definition;

o did not develop a comprehensive certification and accreditation plan to protect DCPDS data and resources;

o did not consider computer security as a criterion to select the commercial software solution to process DCPDS personnel data; and

o did not adequately incorporate information assurance recommendations that subject matter experts provided.

As a result, DCPDS has high risks of unauthorized access to system data and resources; alteration and destruction, whether intentional or not, of personnel data; and denial of service to authorized system users if it fails to adequately safeguard personal and privacy information in accordance with the Privacy Act.

Information Assurance Controls

Federal Guidance. Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996, (the Circular) recognizes the need for special management attention for security of automated information systems because of the risk and magnitude of harm that

could result from the loss, misuse, or unauthorized access to or modification of management information. In addition, the Circular requires agencies to recognize that the individual's right to privacy must be protected in Federal Government information systems involving personal information.

The Circular directs all Federal agencies to protect information commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. The Circular requires agencies to incorporate minimum controls to be included in all Government automated information system security programs. One of those controls is for agencies to assign, in writing, individuals to assure that adequate security exists for the automated information system because of the high risk to major applications. The Circular also requires that those individuals responsible for computer security be technically knowledgeable in the nature of the information and in the controls used to protect it.

DoD Security Requirements. DoD Directive 5200.28 (the Directive) provides mandatory minimum automated information system security requirements for systems that process sensitive-but-unclassified information. The Directive incorporates the provisions of the Circular and requires DoD Components to appoint a designated approving authority (DAA) to be responsible for automated information system security. DoD Standard 5200.28-STD, "Department of Defense Trusted Computer Security Evaluation Criteria, " December 1985, (the Standard) states that the system must enforce an explicit and well-defined security policy so that no individual lacking proper authority can access the system. The Standard requires security policy to reflect the laws, regulations, and general policies from which it is derived. The Defense Information Systems Agency published DoD Instruction 5200.40, "DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997, to provide DoD managers with a unified process to incorporate adequate computer security into their systems. Together, the Directive, the Standard, and the DITSCAP provide DoD managers the framework for adequately safeguarding information and the computer resources that process information.

Minimum **Security Requirements.** The Directive mandates that all systems that process sensitive-but-unclassified information meet minimum security requirements and have either manual or automated safeguards. The Directive states that systems that process sensitive-but-unclassified information must base the security classification level of a system on a risk assessment procedure within the Directive. The risk assessment procedure requires systems that process sensitive-but-unclassified information and that do not transmit data on dedicated communications hardware to meet the minimum requirements of security classification level C-2. The Standard provides criteria for automated information system security classifications and specifies that to meet the requirements of a C-2 level, a system must make its users individually accountable for their actions, must provide auditing of security-related events, and must isolate its resources. A mix of technical, operational, administrative,

and other control mechanisms should achieve the requisite level of protection needed to satisfy the responsibility of DAA for protecting a system's data and computer resources.

System Certification and Accreditation. The DITSCAP requires the following prerequisites for a DAA who is responsible for automated information systems security:

- should be a senior operational commander with the authority and ability to evaluate the operational needs for the system in view of the security risks;

- must have the authority to oversee the operations and use of systems under his/her command; and

- represents the interests of mission need, controls the operating environment, and defines the system-level security requirements.

The DITSCAP does not differentiate between DoD Component and Defense-wide automated information systems in its discussion about the system DAA.

The Directive requires that DAAs base their accreditation decisions on the results of a certification process. The DAA reviews and approves security safeguards, accredits assigned systems, and appoints an official to perform the technical analysis of the system's operational status. The technical analysis, performed by the certification official, will provide decisionmaking information to the DAA regarding the adequacy of system security. The continuous process used by the DAA and the certification official leading up to the accreditation decision is called the certification and accreditation process. The DCPDS DAA is the DoD Technical Implementation Manager, and the certification official is the DCPDS acquisition program manager. Currently, responsibilities of both positions are assigned to the Technical Director, Directorate of Personnel Data Systems, Air Force Personnel Center. See Appendix E for an overview of the DITSCAP.

Information Assurance Progress

The Office of the Director, Information Assurance, Assistant Secretary Defense (Command, Control, Communications, and Intelligence), in coordination with the functional program manager and the acquisition program manager, initiated actions to identify and plan DCPDS information assurance solutions. Beginning in May 1997, representatives of the Director, Information Assurance, coordinated DCPDS information assurance concerns with the functional and acquisition program managers. During October 1997, a computer security response team, led by a representative of the Director, facilitated a risk

assessment process with DCPDS security staff. As a result of the risk assessment process, the acquisition program manager will prioritize DCPDS risks.

Before and during the performance of our audit, the acquisition and functional program managers initiated actions to define and prioritize DCPDS risks. The acquisition program manager requested and obtained a legal opinion from the Air Reserve Personnel Center' on protecting the DCPDS data and provided the Air Force Information Warfare Center with preliminary computer security information. In May 1997, the DCPDS computer systems security officer, a staff manager who reports to the acquisition program manager, chaired the initial DCPDS computer security working group, which included computer security representatives from the DoD Components. Additionally, the acquisition and functional program managers have worked with the Office of the Director, Information Assurance, to assess DCPDS risks and are developing an action plan to mitigate those risks.

Safeguarding DoD Civilian Personnel Records

Despite the measures taken, the DCPDS will not have controls in place to adequately safeguard approximately 750,000 DoD civilian personnel records and the computer resources used to process those records. The DCPDS will contain unclassified information that will be processed in a client-server computing environment. The clients will be computer workstations at the 23 regional personnel servicing centers and at the 300 base-level customer units. The servers will be mini-computers and will be located at the 23 regions. The civilian personnel data will be stored on the servers and transmitted through local area networks and the internet, where necessary. In addition, a corporate computer system will store all civilian personnel records.

The DCPDS data are subject to the provisions of the Privacy Act, which requires automated information systems to protect personal information and records to prevent harm, embarrassment, or inconvenience to the individuals on whom the information pertains. The DCPDS data processing will be performed through a commercial off-the-shelf software application and is expected to be hosted on a variety of computer operating systems. Each computer operating system will have unique security features and each will require a separate evaluation. Protecting or safeguarding that information requires a comprehensive plan that includes the technical controls needed for different computing environments.

'The Staff Judge Advocate, Air Reserve Personnel Center, informed the acquisition program manager that transmission of personnel information on the internet could violate provisions of the Privacy Act and needs to be safeguarded.

Technical controls include computer security measures to:

- prevent unauthorized access to system data and computer resources;
- preserve the integrity of the data; and
- provide availability of system resources to authorized users, when needed.

The DCPDS functional and acquisition program managers jointly prepared a DCPDS security policy and a security support plan. While those security documents provided broad DCPDS security information, the documents did not identify comprehensive system protection mechanisms. For example, those documents did not address how transmissions of DCPDS data would be protected. In addition, those documents did not identify a need for computer hardware safeguards such as tirewalls, but stated that the restriction of access to the system through a password policy and the implementation of audit records of key events would provide adequate system protection.

Functional and Acquisition Program Management Roles

The DCPDS functional and acquisition program managers did not initially recognize or define DCPDS information assurance requirements. The functional and acquisition program managers did not adequately recognize or define system threats during DCPDS requirements definition. In addition, the functional program manager and the acquisition program manager did not initiate a comprehensive, agreed-to security certification and accreditation plan to adequately prepare the system for a favorable accreditation decision. Further, the functional and acquisition program managers did not use computer security features as a criterion to evaluate commercial human resources data processing software alternatives' and did not adequately incorporate information assurance recommendations that subject-matter experts provided to improve DCPDS security.

Security Requirements. The functional and acquisition program managers did not adequately recognize or define system threats during DCPDS requirements definition. The acquisition program manager prepared the operational requirements document for the functional program manager and incorrectly concluded that DCPDS has no perceivable system threats to system design. The acquisition program manager based this conclusion on a belief that, by acquiring security classification C-2 compliant hardware and software, system threats are eliminated. That conclusion is erroneous because system threats will always be

[2]The DCPDS functional and acquisition program management jointly evaluated three commercial human resources software applications from August through September 1995.

present. The use of C-2 compliant hardware and software may offset DCPDS vulnerabilities, which would reduce operational risks, but not system threats. According to the National Information Systems Security Glossary, NSTISSI No. 4009, January 1996, system threats are any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and denial of service. The glossary defines operational vulnerabilities as weaknesses in an information system or components that an individual could exploit; for example, system security procedures, computer hardware design, and internal controls. DoD Directive 5200.28 requires the acquisition program manager to safeguard the DCPDS through the continuous use of security measures consisting of administrative, procedural, physical or environmental, personnel, communications, emanations, and computer security. However, in the case of DCPDS, the acquisition program manager needed a documented functional requirement for protecting DCPDS. By defining system threats, the functional and acquisition program managers will be able to plan for and implement an adequate DCPDS information assurance program.

At the completion of audit verification, representatives of the Major Automated Information Systems Review Council assembled a team of DoD Component and acquisition program manager security experts to conduct a facilitated risk assessment. The risk assessment team identified DCPDS program risks that the acquisition program manager is using to develop a risk assessment action plan. The action plan should be a foundation for DCPDS information assurance.

Comprehensive DCPDS Certification and Accreditation Planning. The DCPDS functional and acquisition program managers did not develop a comprehensive certification and accreditation plan to protect DCPDS. Specifically, the functional program manager created a potential conflict of interest by assigning to the acquisition program manager the responsibility for certifying system compliance with security policy and the responsibility for accrediting DCPDS for operations. Also, the acquisition program manager did not adequately establish and document a system certification plan in the DCPDS security support plan.

DCPDS Certification and Accreditation Responsibilities. On August 21, 1995, the functional program manager assigned certification and accreditation responsibilities to the DCPDS acquisition program manager, creating a potential conflict of interest. According to the DITSCAP, the certification official is responsible for assessing system compliance with the security policy and making recommendations to a DAA. The certification official should be technically knowledgeable about the system and would normally issue a certification to the DAA that the integrated system satisfies agreed-to security requirements. The certification official should be independent of the organization responsible for the system to reduce the potential of conflicts of interest and to permit impartial system evaluation.

The DITSCAP states that a DAA should be an official at an organizational level high enough to be responsible for evaluating the overall mission requirements of

the automated information system. Further, the DAA provides definitive direction to the system developer or owner on the risk in the automated information system security posture. The DAA has authority to accept the security safeguards prescribed, and the DAA can issue an accreditation statement that records the decision to accept the safeguards. It will be difficult for the DCPDS acquisition program manager, as the system DAA and certification official, to maintain the independence necessary to perform system development tasks, system certification tasks, and, ultimately, accept overall security responsibility for DCPDS data and computer resources. Without adequate separation of the duties, the acquisition program manager can define the DCPDS security safeguards, design them into the system, assess the adequacy of the safeguards, modify the safeguards, approve the safeguards, and accredit the DCPDS for operations without independent oversight.

DCPDS Certification and Accreditation Plan. The DCPDS functional program manager and acquisition program manager did not adequately establish and document a system certification plan in the DCPDS security support plan, even though DCPDS is scheduled to begin operations at selected locations within 6 months. The DCPDS program managers recorded security policy and a security support plan, but neither recorded an agreed-to certification and accreditation process for the DCPDS DAA and the certification official. As outlined in the DITSCAP, certification officials need certification plans to document the elements of the certification process.

The DAA needs a certification plan to ensure that the certification official follows a methodical process that the acquisition program manager, the DAA, and the system user's representative agree to, which leads to the DAA accreditation decision. Key elements of a certification plan should include:

- an agreement of the conditions for certification and accreditation among the DAA, the system user's representative, and the system developer or program manager;

- a record of all requirements necessary for accreditation;

- a record of all security criteria for use throughout the automated information system's life cycle; and

- a record of the certification process.

The DCPDS acquisition program manager and the functional program manager approved an incomplete DCPDS security support plan to serve as the certification and accreditation plan. The plan was flawed because it allowed the certification and accreditation responsibilities to reside with a single official and omitted information to describe certification and accreditation procedures. The plan does not describe how the certification official will evaluate the security

features, whether the certification official will perform a risk analysis, or how the certification official will validate security policy requirements. The DCPDS functional and acquisition program managers and a DAA need to approve a comprehensive certification and accreditation plan that will provide a basis for protecting the system data and computer resources.

DCPDS Commercially Procured Software. The DCPDS functional and acquisition program managers recommended a commercial software alternative, but they did not include information assurance as a criterion for comparison when selecting the software. The Directive requires that statements of security requirements be included in the acquisition and procurement specifications for automated information systems. The statements should be based on the results of an initial risk assessment and should specify the system's security classification level, as required by the Standard. The acquisition program manager performed a draft technical analysis of three potential commercial software applications in August 1995 but did not evaluate security. The functional and acquisition program managers used that technical analysis and other factors to rate the three software applications. The results of the ratings led to a September 29, 1995, Deputy Assistant Secretary of Defense (Civilian Personnel Policy) memorandum directing the acquisition program manager to initiate contract negotiations for one of the alternatives. Accordingly, the DCPDS functional and acquisition program managers did not adequately evaluate the security features of commercial software alternatives and should include computer security statements in all future contracting actions for DCPDS, where applicable.

Technical Advisors. The DCPDS acquisition program manager did not adequately incorporate official advice and recommendations from expert security officials of the Defense Information Systems Agency, the Air Force Communications Agency, the Air Force Information Warfare Center, and the National Security Agency. Security analysts in those organizations have worked closely with DCPDS officials since early 1996 and provided comments and advice on how to protect sensitive-but-unclassified DCPDS data. The DCPDS security officials were nonresponsive to the advice and recommendations that security experts from other DoD organizations made. DCPDS security officials could not adequately document the system security policy for Defense Information Systems Agency officials, could not define the DCPDS technical architecture in detail to system testers of the Air Force Information Warfare Center to plan security testing, and refused to consider technical security solutions that the system needs to meet legal obligations of DoD to protect individual privacy rights because of the lack of budgeting for the cost of the solutions. We recognize that the acquisition program manager has a responsibility to complete the DCPDS development within cost, schedule, and performance requirements, yet the acquisition program manager should incorporate the advice and recommendations provided by the organizations listed previously because the recommendations are similar to recommendations

in the acquisition program manager's draft initial risk assessment[3] and because those officials recognize the need to protect DoD assets in the aggregate. The acquisition program manager's draft initial risk assessment concluded that significant DCPDS computer security risks existed that need to be reduced.

DCPDS Security Risks

The DCPDS program has high risks for unauthorized access to DCPDS system data and resources; alteration and destruction of personnel data, whether intentional or not; and denial of service to authorized system users. In addition, by not adequately protecting DCPDS, the acquisition program manager introduces additional security risks for directly and indirectly connected DoD computer systems, which comprise the Defense Information Infrastructure. The DoD Major Automated Information Systems Review Council reviewed the DCPDS information assurance program, but it had not been able to ensure that DoD civilian personnel data and the resources used to process and transmit those data have been adequately safeguarded.

Confidentiality, Integrity, and Availability of Civilian Personnel Data. The acquisition program manager has the responsibility to ensure that DCPDS will provide the confidentiality, integrity, and availability needed for successful civilian personnel data processing. The Computer Security Act requires agencies to protect personal information, such as DoD civilian personnel data, from disclosure to unauthorized individuals. The DCPDS security policy states that the confidentiality of civilian personnel data will be protected through the enforcement of controlled access to the system through user passwords. However, the DCPDS draft initial risk assessment states that the core DCPDS commercial application did not have adequate password features. In addition, the security policy does not state how controlled access at all levels of DCPDS operations will be accomplished, or whether different access controls are needed for DCPDS computer resources that process other mission requirements of the DoD. The draft initial risk assessment also identified that no security techniques were in place to protect the confidentiality of DCPDS data transmitted over the local communications networks or the internet. Inadequate protection of access to the system increases the risk of compromise to the accuracy (integrity) of the data and the availability of the system when needed.

Additional Risks. DoD oversight officials need timely and accurate computer security information from the DCPDS acquisition program manager to evaluate the overall risk that DCPDS adds to the Defense information infrastructure. Inadequate DCPDS computer security safeguards create risks for other DoD

---

[3] The DCPDS initial risk assessment has remained in draft form since December 1995. The acquisition program manager did not perform a more recent DCPDS risk assessment.

systems that are connected directly or remotely with DCPDS resources. The DoD Major Automated Information Systems Review Council is responsible for evaluating the systems within the context of that infrastructure.

The DCPDS quarterly reports that are used by the Major Automated Information Systems Review Council to evaluate program progress omitted details on computer security issues and the potential resource impacts that computer security solutions posed. The DCPDS acquisition program manager continually reported computer security as an area that would not impact cost, schedule, or performance, yet the acquisition program manager stated that computer security was not thoroughly planned or budgeted. Because DCPDS will provide direct connections to at least six other DoD automated information systems, the DoD Major Automated Information Systems Review Council should consider the adequacy of DCPDS computer security in relation to other DoD systems.

Potential Legal Liability. Potential legal liability exists for DoD if civilian personnel data are not adequately safeguarded. The Privacy Act requires, among other things, that agencies "... establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated system threats or hazards to their security or integrity, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." A civil remedy is available to an aggrieved party when an agency fails to comply with a provision of the Act, or the rules promulgated in it, in a way that has an adverse effect on that individual. The DoD could, in an appropriate case, be liable for the actual damages sustained, plus costs and attorneys' fees.

Because the DCPDS will process personal and private information maintained in DoD civilian personnel records and will use nonsecure communications to transmit that information, we believe that the system requires adequate protective measures to reduce the potential for harm to employees and to reduce the potential for civil liability to the DoD.

Conclusion

The functional and acquisition program managers have initiated actions to define and prioritize DCPDS risks. However, the functional and acquisition program managers did not adequately recognize or define system threats during DCPDS requirements definition and did not develop a comprehensive certification and accreditation plan to protect DCPDS. Also, the functional and acquisition program managers did not include information assurance as a criterion for comparison when selecting the software. Without incorporating information assurance into the DCPDS development process, the acquisition program manager will not provide the confidentiality, availability, and integrity required to process sensitive-but-unclassified data on the DCPDS. The DCPDS

Milestone Decision Authority, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), should coordinate with the Office of the Assistant Secretary of the Air Force (Acquisition) and the Civilian Personnel Management Service to determine and assign responsibility for DCPDS safeguards. We directed some recommendations to the Commander, Electronics Systems Center, Air Force Materiel Command, because the Commander provides acquisition management and direction to the DCPDS acquisition program manager.

Management Comments on the Finding and Audit Response

Civilian Personnel Management Service Comments on the Finding. The Director, Civilian Personnel Management Service (CPMS), agreed that civilian personnel data should be safeguarded and that the DCPDS certification and accreditation plan was inadequate. The Director disagreed with our conclusions that the DCPDS operational requirements document was prepared incorrectly, the assignment of certification and accreditation responsibilities created a conflict of interest, and the DCPDS human resources commercial software acquisition was improper.

The Director revised our estimates of DCPDS life-cycle costs, stating DCPDS investment costs to be about $350 million and life-cycle costs to be about $795 million. The Director noted that our report overstated life-cycle costs by including personnelists' salaries.

The Director also provided current DCPDS schedule information, stating that the DCPDS initial operational capability is scheduled for June 1998 and full operational capability is scheduled for September 1999.

Audit Response. CPMS was proactive in implementing our recommendations. As a result of management actions taken or planned, we changed report information regarding DCPDS costs and schedule and revised our discussions about system threats. Our responses to CPMS comments on specific issues follow.

Operational Requirements Document. The Director disagreed with our conclusions that the DCPDS operational requirements document was prepared incorrectly, stating that we misinterpreted the language of the document. The Director stated that the term "no perceivable threats" was used in the operational requirements document in the context that by acquiring C-2 compliant system hardware and software, the DCPDS processing environment would have no perceivable system threats that must be countered by system design. Finally, the Director stated that the acquisition program manager is developing a DCPDS risk assessment action plan based on risks identified by a computer security response team in October 1997.

Audit Response. CPMS comments on the operational requirements document were partially responsive. We concluded the document was inadequate because the acquisition program manager did not adequately identify system threats during requirements definition and that, without defined system threats and an analysis of system vulnerabilities, the acquisition program manager would find it difficult to determine the needed safeguards. The risk assessment action plan under development by the DCPDS acquisition program manager should address our concerns. We request that CPMS provide milestones for the completion of the risk assessment action plan in its comments on the final report.

Certification and Accreditation Plan. The Director generally agreed with our conclusions that the DCPDS certification and accreditation plan was inadequate but stated that the plan complied with DoD Directive **5200.28.** The Director noted that on the basis of our report, a more comprehensive certification and accreditation plan was being prepared.

Audit Response. CPMS comments on the certification and accreditation plan were responsive, and planned management action should correct the identified weaknesses. We request that CPMS provide milestones for completion of the certification and accreditation plan in its comments on the final report.

Assignment of Certification and Accreditation Responsibilities. The Director disagreed with our conclusions that assignment of certification and accreditation responsibilities created a conflict of interest. The Director stated that no conflict of interest exists regarding the assignment of certification and accreditation responsibilities to the developmental DAA. The Director agreed, however, that the duties of the DCPDS certification official and the DAA need to be separated and stated that the CPMS will appoint an operational DAA before the completion of the certification and accreditation plan. The acquisition program manager will not be both the system DAA and the certification official.

Audit Response. We disagree with the comments that separation of duties is not needed for the developmental DAA; however, planned management actions meet the intent of that recommendation. We request that CPMS provide milestones for appointment of the operational DAA in its comments on the final report.

Commercial Software Acquisition. The Director disagreed with our conclusions the DCPDS human resources commercial software acquisition was improper, stating that the acquisition program manager used security as a criterion during a preliminary draft technical assessment of three commercial products.

Audit Response. CPMS comments were partially responsive. We agree that a draft preliminary technical analysis included security standards of the DoD Technical Architecture Framework for Information Management, but management did not analyze the effects on system security of each package under consideration. Because the selection of software has already been made, no further comments are required.

Air Force Comments on the Finding. The Air Force stated that the acquisition program manager has maintained a close relationship with security experts in DoD and Federal organizations and has incorporated many of their suggestions and recommendations. The DCPDS acquisition oversight integrated process team evaluated computer security and requested DoD to provide additional guidance regarding encryption. The Air Force was proactive in implementing our recommendations. The Air Force disagreed with the statements that the DCPDS commercial software acquisition did not consider computer security and that the acquisition program manager did not incorporate information assurance advice from technical experts. The Air Force stated that the acquisition program manager recommended a DCPDS commercial software solution based on a draft preliminary technical analysis that included computer security.

Audit Response. Comments from the Air Force were responsive. We do not agree with management comments that the acquisition program manager has maintained a close relationship with security experts in the organizations mentioned; however, the acquisition program manager's actions to protect DCPDS have improved. According to representatives of the organizations mentioned, the acquisition program manager's assignment of an information systems security officer has resulted in a dramatic increase in cooperation among the organizations. Because of those actions, no further comments are required.

Recommendations, Management Comments, and Audit Response

Deleted and Renumbered Recommendations. As a result of the comments, we eliminated draft Recommendation 2.a. to revise the operational requirements document and renumbered the remaining two recommendations as 2.a. and 2 .b. Also, we revised draft Recommendation 2.b. because the Civilian Personnel Management Service needs to communicate functional security requirements with acquisition management.

1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

a. In coordination with the Director, Civilian Personnel Management Service, and the Commander, Electronics Systems Center, Air Force Materiel Command, assign a single overall designated approving

authority for the Defense Civilian Personnel Data System program consistent with provisions in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988.

b. Include in oversight reviews of applicable DoD automated information systems the risks that the Defense Civilian Personnel Data System information assurance program adds to the interconnected systems.

Management Comments Required. The Assistant Secretary did not comment on a draft of this report. We request that the Assistant Secretary provide comments on the final report by March 23, 1998.

2. **We recommend that the Director, Civilian Personnel Management Service:**

a. Provide a functional statement of security needs to the Defense Civilian Personnel Data System acquisition program manager.

b. Coordinate with the acquisition program manager and the designated approving authority to approve a certification and accreditation plan to protect the Defense Civilian Personnel Data System.

Management Comments. The Director concurred with Recommendation 2.b. (draft Recommendation 2.c.). The Director nonconcurred with Recommendation 2.a. (draft Recommendation 2.b.), but actions taken and planned meet the intent of the recommendation.

Audit Response. As a result of the comments, we deleted draft Recommendation 2.a. and revised and renumbered the remaining two recommendations as Recommendations 2.a. and 2. b.

3. **We recommend that the Commander, Electronics Systems Center, Air Force Materiel Command, direct the acquisition program manager to develop a comprehensive certification and accreditation plan for the Defense Civilian Personnel Data System that:**

a. Defines computer security measures to minimize the high risks and the magnitude of harm or loss.

Management Comments. The Air Force concurred and stated that the acquisition program manager would prepare an information protection document that would define the computer security measures to minimize system risks by January 1998.

b. Includes computer security requirements in contract solicitations or other instruments for the Defense Civilian Personnel Data System to

comply with requirements of DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, where applicable.

Management Comments. The Air Force concurred and stated that it will consider computer security requirements in further contract solicitations, although it has not planned any further acquisition decisions.

c. **Incorporates applicable recommendations made by technical experts on protection needs for DoD civilian personnel data and computer resources used to process those data.**

Management Comments. The Air Force concurred and stated that the Civilian Personnel Management Service developed an action plan as a result of a joint security effort in October 1997. Also, the Air Force stated that the Computer Security Working Group will have increased DoD Component representation, which will enhance security policy recommendations and technical proposals. A joint test team from the acquisition program management staff and the Air Force Information Warfare Center will evaluate the technical suitability of encryption solutions.

d. Appoints a certification official independent of and accountable to the Defense Civilian Personnel Data System designated approving authority.

Management Comments. The Air Force concurred and stated that the functional program management staff will appoint a certification official during January 1998.

e. **Has agreement of the designated approving authority and the functional system proponent or representative.**

Management Comments. The Air Force concurred and stated that the functional program management staff is currently preparing a certification and accreditation plan to be completed during January 1998.

Management Comments on Management Controls

The Air Force agreed that management's self evaluation did not identify the DCPDS program or the computer security as an assessable unit, As a result, the Air Force added an assessable unit to the 5-Year Management Plan.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

We reviewed DCPDS functional and acquisition program documentation, contract actions, and organizational guidance dated from FYs 1988 through 1997 to support the information assurance planning process used for developing the modernized DCPDS. Specifically, we reviewed DCPDS program planning documents such as the initial risk assessment, the security support plan, concepts of operation, the operational requirements document, the communications support plan, the test and evaluation master plan, and the security policy. We conducted interviews and held discussions with the functional and acquisition program managers' staff. We also conducted interviews and held discussions with Air Force Personnel Center staff in the areas of personnel systems' security, contract management, and hired contract personnel regarding DCPDS procurements as they related to information assurance. We did not rely on computer-processed data to accomplish the overall audit objective.

Scope Limitation. We did not perform a vulnerability analysis and assessment to determine the security risk associated with civilian personnel information processed at the various DoD Components. The Army and Air Force Audit Agencies performed those analyses and assessments in coordination with the Army Land Information Warfare Activity and the Air Force Information Warfare Center.

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

Audit Period, Standards, and Locations. We performed this economy and efficiency audit from January through October 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.

Management Control Program

DoD Directive 5010.38, "Management Control (MC) 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 the Management Control Program. We reviewed the management controls as they relate to the DCPDS information assurance program. Specifically, we reviewed the Air Force Personnel Center management controls for planning, implementing, and validating computer security for DCPDS. We reviewed management's self-evaluation applicable to those controls.

Adequacy of Management Controls. We identified material management control weaknesses for the Directorate of Personnel Data Systems, Air Force Personnel Center, as defined by DoD Directive 5010.38. Air Force Personnel Center controls for information assurance were inadequate to ensure the confidentiality, integrity, and availability of the information stored on and processed by the DCPDS. Also, the Technical Director, Directorate of Personnel Data Systems, Air Force Personnel Center, was assigned to perform responsibilities of security officials, which are normally separate. Recommendations 1., 2., and 3.d., if implemented, will improve the controls for protecting the DCPDS. A copy of this report will be provided to the senior official responsible for management controls at the Air Force Personnel Center.

Adequacy of Management's Self-Evaluation. Management's self-evaluation did not identify the DCPDS program or the computer security as an assessable unit and, therefore, did not identify or report the material management control weaknesses identified by the audit. However, management did identify concerns for DCPDS computer security and provided an audit suggestion to the Inspector General, DoD.

Appendix B. Summary of Prior Coverage

General Accounting Office

GAO Report No. AIMD-96-144 (OSD Case No. 1213), "DoD General Computer Controls: Critical Need to Greatly Strengthen Computer Security Program," September 30, 1996. The report discusses the General Accounting Office evaluation of the general computer controls at several large Navy and Marine Corps computer installations and at selected Defense Information Systems Agency Defense Megacenters. The report notes security weaknesses that would allow hackers and legitimate users to improperly access, modify, or destroy sensitive DoD data. The report recommended a centralized security management program with defined responsibilities, periodic reviews, and monitoring and reporting of improvement actions. DoD management concurred with all findings and recommendations.

GAO Report No. AIMD-96-84 (OSD Case No. 1150), "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," May 22, 1996. The report discusses the General Accounting Office review of the extent to which DoD computers are being attacked, the potential for damage, and the challenges faced in responding to the attacks. The General Accounting Office notes that attacks are increasing, damaging, and a threat to national security. The General Accounting Office concludes that policies are out-of-date and inconsistent, and that many users are not aware of the magnitude of the problem. The report recommended that the Secretary of Defense strengthen the DoD information systems security program by improving policies and procedures, increasing user awareness, setting standards, monitoring security, and establishing responsibility and accountability. DoD management agreed with the report's findings and recommendations.

Office of the Inspector General, DoD

Inspector General, DoD, Report No. 98-024, "Security Controls Over Systems Serving the DoD Personnel Security Program," November 19, 1997. The audit objective was to evaluate security controls over the computer system serving the DoD personnel security program, which the Defense Investigative Service administers. The report states that the Defense Investigative Service did not have adequate controls to protect personnel security systems and data from compromise. Therefore, the Defense Investigative Service has no assurance that unauthorized individuals cannot access, modify, or destroy the highly sensitive DoD personnel security

information that the Defense Investigative Service administers. The Inspector General, DoD, recommended the Defense Investigative Service to communicate specific security requirements, modify Memorandums of Agreement and contracts to include system security, develop and implement access control policies, isolate critical resources in the system architecture, and improve physical security. Defense Investigative Service management agreed with all recommendations and had initiated actions to improve systems security and the systems architecture.

Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," September 25, 1997. The audit objective was to determine the effectiveness of DoD management of information assurance efforts to protect automated information systems. The report concludes that DoD needs to improve the security safeguards and practices to protect the DoD automated information systems that process sensitive-but-unclassified information from unauthorized access. Inefficient and ineffective implementation of the Defense-wide Information Systems Security Program, outdated policies and procedures, inadequate direction and oversight, and lack of accountability for information systems security management controls contributed to the inadequate security safeguards. The Inspector General, DoD, recommended developing procedures to determine the Defense Information Infrastructure's security posture, developing an information assurance strategic plan, and incorporating accountability requirements for personnel responsible for safeguarding DoD automated information systems. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) generally concurred with the recommendations and is establishing an integrated management process to extend DoD oversight of information assurance programs and activities to all DoD Components. Policy will be established to standardize the security certification and accreditation process for information technology. In addition, DoD-wide programs will be established for information security assessments and reviews and for incident reporting and response.

Air Force Audit Agency

Project No. 96054027, "Data Communications Security," April 15, 1997. The audit objective was to determine whether the Air Force adequately protects sensitive-but-unclassified information transmitted over the Air Force Internet. The report concludes that Air Force systems continued to transmit sensitive-but-unclassified information unprotected over the Air Force Internet because the Air Force system managers had not conducted a risk analysis. Users and system managers of 5 of the 11 systems examined were not aware of the increased risk of using the Air Force Internet or of the sensitive nature of the information. The Air Force Audit Agency recommended a risk analysis for

each system that identifies the current risks of transmitting sensitive-but-unclassified information over the Air Force Internet, as well as emphasizing protection requirements to the designated approval authorities. Air Force management officials agreed with the overall audit results and planned responsive actions.

Project No. 93058001, "Review of Personnel Concept III System Security and Equipment Management, " April 3, 1995. The audit objective was to determine whether selected security and control procedures were properly implemented in the Personnel Concept III computer system. The report concludes that the Air Force did not implement adequate security access protection for the system and did not properly account for computer equipment. The Air Force Audit Agency recommended implementing separating requirements, maintaining consolidated accreditation data bases, identifying system threats and areas requiring additional protection, and implementing proper control and authorization of passwords. Air Force management officials agreed with the overall audit results and planned responsive actions.

Other Related Coverage

Defense Science Board Task Force, "Information Warfare-Defense (IW-D)," November 21, 1996. The task force was established to study the protection of information interests of national importance through a credible information warfare defensive capability. The report concludes that DoD needs to defend against possible information warfare attacks against DoD systems that could impact the ability of DoD to carry out its responsibilities. The task force recommended 50 actions, ranging from identification of a focal point within DoD for information warfare activities to allocation of approximately $3 billion over the next 5 years to implement recommendations.

Joint Security Commission, "Redefining Security," February 28, 1994. The Joint Security Commission report addresses the processes used to formulate and implement security policies in DoD and the intelligence community. The Joint Security Commission concluded that the clearance process is needlessly complex, cumbersome, and costly. The Joint Security Commission made recommendations that would create a new policy structure, enhance security, and lower cost by avoiding duplication and increasing efficiency.

Appendix C. Other Matters of Interest

Interim Certification of Air Force Personnel System

The Air Force civilian personnel data processing system does not have controls in place to protect civilian personnel information or the resources used to process that information. On April 21, 1997, the Director of Personnel Data Systems, Air Force Personnel Center, granted interim accreditation for Air Force regional service centers to process civilian personnel data on the "Palace Compass" data processing application and its resources, subject to provisions in Air Force Policy Directive 33-2, "Information Protection," December 1, 1996. The Palace Compass data processing is the interim Air Force system used to process civilian personnel data until the modernized DCPDS becomes operational. The modernized DCPDS may use some of the Palace Compass data processing resources.

Basis. The interim accreditation increases risks to DCPDS because plans and procedures are not in place to protect the confidentiality and integrity of the data and to ensure the availability of the system. According to the accreditation memorandum, the Director granted interim authority to Air Force organizations to operate the Palace Compass data processing because:

o processing that information was so critical that security measures and safeguards could be deferred until the complete DCPDS is deployed;

o the transition process to an accredited DCPDS is outlined in the DCPDS modernization program deployment schedule and plan; and

o the technical considerations of the system warrant an interim accreditation.

The certification and accreditation documentation did not support the interim accreditation decision. We did not audit the Palace Compass data processing, but reviewed the certification and accreditation documentation to determine whether DCPDS data and resources were adequately protected. The transition process outlined in DCPDS documents does not provide any assurance that current civilian personnel information is being adequately safeguarded. In addition, the technical considerations of the Palace Compass data processing system were not documented in a risk analysis or in any other program plans that the DAA could use to certify and accredit DCPDS. The accreditation decision states that Palace Compass security measures provided by the Palace Compass applications are adequate. The accreditation documentation further states that security officials at each Palace Compass operational site should use

guidelines in the DCPDS security policy. The guidelines are not included in the accreditation documentation; therefore, Palace Compass data processing resources may not have appropriate safeguards to protect existing civilian personnel action processing.

DCPDS Modernization Deployment Schedule and Plan. The April 22, 1997, draft DCPDS Modern System Deployment Plan (the Plan) identifies requirements to transition current (interim) civilian personnel data processing resources to DCPDS but does not present a DCPDS certification and accreditation plan. The Plan identifies the need to protect the modernized DCPDS and its data, and it references the DCPDS security support plan. The reference from the Palace Compass accreditation memorandum to the DCPDS modernization deployment schedule that refers to the DCPDS security plan does not provide assurance that existing DCPDS resources are adequately protected or that they will be adequately protected in the future.

Technical Considerations. The DCPDS technical considerations were inadequate to support a basis for interim accreditation of the Palace Compass data processing system. According to the Director, Directorate of Personnel Data Systems, Air Force Personnel Center, the accreditation decision was supported by a risk assessment and a concept of operations. The Civilian Personnel Management Service had not incorporated validated system threats into DCPDS requirements, and DCPDS security officials did not have a complete certification and accreditation plan. As of April 21, 1997, the DCPDS acquisition program manager had not developed a concept of operations. In addition, the DCPDS acquisition program manager had not documented system threats, vulnerabilities, recommendations for countermeasures to vulnerabilities, and other technical risks normally identified in a risk assessment, although that information was available in December 1995 through a draft initial risk assessment. Further, on April 14, 1997, the Air Force Operational Test and Evaluation Center reported that moderate risk existed to test and deploy DCPDS in a timely manner. Specifically, the center reported that insufficient information was available for developmental increments, developmental testing data, program documentation, and program schedule. The center was not tasked to review the technical aspects of DCPDS, such as computer security features.

Protection of Privacy Act Information. The Director stated that current Air Force civilian personnel data processing functions are operating without a plan to define the level of protection needed for the system. However, the Director did not recognize the need to protect the civilian personnel data in consonance with the Privacy Act or the exemption provisions of the Freedom of Information Act. The interim accreditation places the privacy of the data and the operations of the resources used to process the data at risk.

Appendix D. Glossary

Federal and DoD organizations have published numerous definitions for terms to describe conditions, events, and key officials involved with safeguarding automated information systems. We primarily used definitions from DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, and other guidance.

Accreditation. Accreditation is a formal declaration by a DAA that a system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operating an automated information system and is based on the certification process as well as on other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. ***(DoD*** Directive 5200.28)

Availability. Availability is the condition when information stored or processed on a system is not denied to those granted formal access to the data. ***(DITSCAP)***

Certification. Certification is a comprehensive evaluation of the technical and nontechnical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. *(NSTISSI No. 4009)*

Certification Official. The certification official is responsible for reporting the results of the comprehensive evaluation of the technical and nontechnical security features of an automated information system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meet a set of specified security requirements. ***(DITSCAP)***

Confidentiality. Confidentiality is the assurance that information is not disclosed to unauthorized entities or processes. ***(NSTISSI*** *No. 4009)*

Data Integrity. Data integrity exists when data are unchanged from their source and have not been accidentally or maliciously modified, altered, or destroyed. *(NSTISSI No. 4009)*

---

*National Security Telecommunications and Information Systems Security Instruction.

Designated Approving Authority. The DAA is an official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA must be at the organizational level, have authority to evaluate the overall mission requirements of an information system, and provide definitive directions to automated information system developers or owners about the risk in the security posture of the system. ***(DoD** Directive 5200.28, NSTISSI 4009, and DITSCAP)*

Nonrepudiation. Nonrepudiation is assurance of the true identity of participants in a communications exchange. *(NSTISSI No. 4009)*

Security Mode. The security mode is a description of the conditions under which an information system operates, based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. The four modes of operations are the dedicated mode, the system-high mode, the compartmented or partitioned mode, and the multilevel mode. *(NSTISSI No. 4009)*

Threat. A threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, or denial of service. *(NSTISSI No. 4009)*

Vulnerability. A vulnerability is a weakness in an information system or its components (system security procedures, hardware design, or management controls) that could be exploited. *(NSTISSZ No. 4009)*

Appendix E. Certification and Accreditation Process

Developing a Standard Process

In a memorandum dated July 9, 1990, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) directed the Defense Information Systems Agency to develop a Defense-wide information systems security program to coordinate and maintain an integrated information security target architecture for all networks and multilevel secure information systems. In response, the Defense Information Systems Agency prepared an action plan that provided for security initiatives that included institutionalizing security in the system development process. Further, the plan established a program to develop and incorporate information security safeguards into the DoD architecture, and created standardized requirements and processes for accreditation of computers, systems, and networks. Accreditation of the systems and networks is considered a formal declaration by the DAA that an automated information system is approved to operate using a prescribed set of safeguards. The accrediting process is described in DoD Instruction 5200.40, "DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997.

DITSCAP

The DITSCAP defines a process that standardizes all events leading to successful accreditation. The primary purpose of the process is to protect and secure the activities comprising the Defense Information Infrastructure.

That infrastructure includes information resources of DoD Components that will enable personnel data processing to be distributed. The DITSCAP reiterates the minimum security requirements of DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," which requires all DoD automated information systems to be accredited. DoD security officials who follow the DITSCAP will be able to determine the degree of assurance that is needed to achieve security confidentiality, integrity, availability, and accountability of an automated information system.

Certification and Accreditation

The DITSCAP established Defense-wide procedures for officials to certify and accredit automated information systems. DoD Directive 5200.28 requires the DAA to be responsible for implementing the certification and accreditation process and, ultimately, for accepting the risks of an automated information system. The DITSCAP defines the following four phases consistent with system development events to assist DAAs with their responsibilities: definition, verification, validation, and post accreditation.

The definition phase records a baseline of the automated information system, its security requirements, and the people responsible for implementing the requirements. Completion of the definition phase culminates in a formal agreement among the DAA, the acquisition program manager, and the user's representative. The agreement specifies the level of security that the officials require the automated information system to maintain and should be made before the system is developed. The remaining phases build on the agreement.

Key Officials

DoD Directive 5200.28 defines the responsibilities of key officials that affect automated information systems security. The Directive separately lists the responsibilities of a DAA, a user's representative, and an automated information system developer. The DITSCAP also describes the importance of the individual roles and responsibilities of the key officials and introduces the certification official as the technical advisor to the DAA. The three key officials approve the system security authorization agreement, which binds all parties to security requirements needed for system accreditation and records the plan to achieve the accreditation decision. The certification official evaluates the compliance level of the system to the agreement and provides recommendations for improving security features or accepting the system with its risks to the DAA.

Designated Approving Authority. DoD Directive 5200.28 requires DoD Components to appoint DAAs to be responsible for an automated information system's security. The DAA, upon signing the accreditation statement, is responsible for the adequate protection of a system's resources. The DITSCAP requires the DAA to appoint a technical official to evaluate the system's compliance with its security policy. According to the DITSCAP, the DAA should be an official at an organizational level responsible for evaluating the overall mission requirements of the automated information system. Further, the DAA provides definitive directions to automated information system developers or owners about risks of automated information system security features. Also, the DAA has authority to accept or reject the security safeguards that the certification official declares to be present in the system.

User's Representative. The DITSCAP states that the user's representative validates and defines system performance, system availability, and functional requirements.

Automated Information System Developer. The DITSCAP states that the system developer ensures that security requirements are integrated into the automated information system architecture to minimize risks; develops technical requirements; and designs, procures, deploys, and maintains the system.

Air Force Certification and Accreditation Process

The Air Force Communications Agency published policy for managers to use to protect automated information systems. Air Force System Security Instruction 5 102, "The Computer Security (COMPUSEC) Program, " September **23,** 1996, states that controls are needed to validate security events, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of automated information system events, and report incidents. Instruction 5102 states that the DAA is to establish standardization of controls for requirements, system threats, vulnerabilities, level-of-protection, deficiencies, acquisition, accreditation, measures, and reporting of automated information system events. Instruction 5102 also states that the designation of the DAA is one of the most important information protection decisions because the DAA has overall automated information system security responsibility. The DAA also has the authority to remove any system from the network when the system does not adhere to the security requirements. Also, the Air Force Communications Agency published Air Force System Security Instruction 5024, Volume I, "The Certification and Accreditation (C&A) Process," April 1, 1997, to implement the DITSCAP.

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
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 (Force Management Policy)
  Deputy Assistant Secretary of Defense (Civilian Personnel Policy)
    Director, Civilian Personnel Management Service
Assistant Secretary of Defense (Public Affairs)
Deputy General Counsel

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
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 (Acquisition)
Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Commander, Electronics Systems Center, Air Force Materiel Command
Commander, Air Force Personnel Center

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
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 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

THIS PAGE INTENTIONALLY LEFT BLANK

Part III - Management Comments

Civilian Personnel Management Service Comments

DEPARTMENT OF DEFENSE
CIVILIAN PERSONNEL MANAGEMENT SERVICE
1400 KEY BOULEVARD
ARLINGTON, VA 22209-5144

DEC 3 1 1997

MEMORANDUM FOR DIRECTOR, READINESS AND OPERATIONAL SUPPORT DIRECTORATE, OFFICE OF INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Proposed Audit Report on Information Assurance of the Defense Civilian Personnel Data System (Project No. 7RE-3006.01)

As requested by your memorandum of October 30, 1997, the CPMS response to the applicable findings and recommendations of the subject proposed audit report is attached. We share your strong belief that civilian personnel data should be safeguarded and had already taken many appropriate steps before the audit began. We appreciate the opportunity to comment on the proposed report.

Earl T. Payne
Director

Attachment:
As stated

Final Repo
Reference

Functional Management Response

Draft Proposed Audit Report on Information Assurance
Of the Defense Civilian Personnel Data System (DCPDS)
DoDIG Project No. **7RE-3006.01**

AUDIT BACKGROUND

Page 2

Revised

Defense Civilian Personnel Data System (page 3). "...Although a complete program cost estimate is *not* available, the Civilian Personnel Management Service estimated in a September 29, 1997, Economic Analysis, DCPDS program life cycle costs to be about **$795** million. The Civilian Personnel Management Service also estimated total Human Resources mission area cost including the DCPDS life-cycle program costs to be about **$10.3** billion, with total benefits of $2.3 billion. The DCPDS initial operational capability is scheduled for February 1998, and full operational capability is scheduled for June 1999."

Response: with changes.

We request that this paragraph be replaced with the following: ".. .CPMS completed an initial Economic Analysis of the **DoD** Regionalization and Systems Modernization **(Reg/Mod)** Program on January **17, 1996.** Subsequently, CPMS submitted an updated **Reg/Mod** Economic Analysis to the MAISRC on September **29, 1997.** This analysis estimated the **Reg/Mod** investment cost to be about $350 million **and** program life cycle cost to be about $795 million. Savings to be derived **from** the reduction in human resources staff, which the **Reg/Mod** environment facilitates, are estimated to be about $2.3 billion, The Acquisition Integrated Process Team **(IPT)** established a Cost IPT, under the direction of OASD (PA&E), to determine independently a coordinated cost position for each Component transferring from the legacy DCPDS to the modern DCPDS. The Component Cost Position will be used to validate and update the CPMS **Reg/Mod** Economic Analysis. Additionally, the Air Force Cost Analysis Agency is performing a sufficiency review of the **software** development costs for the modem DCPDS. The modem DCPDS initial operational capability at selected test sites is scheduled for June 1998. The modem DCPDS is scheduled to begin full-scale deployment in January 1999 and achieve full operating capability by September 1999."

The cost change is an update based upon the recent **Reg/Mod** Economic Analysis. The schedule change is based upon a revised modem DCPDS schedule presented to the Acquisition IPT on November 12, 1997. "DCPDS life-cycle program costs to be about $10.3 billion" has been dropped because this figure includes not only the life-cycle costs but also the cost associated with the salaries of **personnelists** performing personnel work in the Department. Adding the personnelists' salaries **is in conflict with** OMB **A-109.5.a,** which defines life-cycle costs as "the sum total of the direct, indirect, recurring, nonrecurring, and ***other*** related costs incurred, or estimated to be incurred, in the design, development, production, operation, ***maintenance*** and support of tbe ***major*** system ***over its useful*** life span."

Final Report Reference

Page 8 Revised

FUNDTIONAL AND ACQUISITION PROGRAM MANAGEMENT ROLES

Operational Requirements (page 9). "The acquisition program manager prepared the operational requirements document and incorrectly stated that DCPDS has no perceivable threats."

Response: Nonconcnr.

In February 1996, CPMS met with functional and technical representatives **from** the Military Departments and Defense agencies **(DoD** Components) to validate current functional requirements and identify emerging ones for the modem DCPDS. The CPMS Functional Program Manager **(FPM)** consulted with the modem DCPDS Acquisition Program Manager **(APM)** and key **MAISRC** representatives on the format and content of the operational requirements document (ORD). In July 1996, CPMS completed the ORD. Subsequently, CPMS coordinated the ORD through the modem DCPDS APM and the Deputy Assistant Secretary of Defense (Civilian Personnel Policy) for signature by the Assistant Secretary of Defense for Force Management Policy (ASD (FMP)). The ASD **(FMP)** signed the ORD on October 3, 1996.

The phrase "there are no perceivable threats" appears to have been taken out of context. The ORD. approved on October **3, 1996,** states that "A variety of threats endanger DCPDS survivability. These include typical operating environment threats (e.g., power or air conditioning failure) and natural disasters (e.g., fire and flood). These are countered by the standard physical and procedural requirements consistent with the environment it supports. Trusted agent screening and personal integrity must be **relied** upon to prevent modification or destruction of data, either inadvertent or through means such as **network** monitoring or hacker attacks, that could result in **misuse** or disclosure of sensitive personnel data. By acquiring system hardware and **software** with capability to provide C-2 level system security, there are no perceivable threats, which need to be countered by system design." While the term no ***perceivable threats*** is used in this paragraph, **it** is used in the context that by acquiring C-2 compliant system hardware and **software** there would be no perceivable threats in the modem DCPDS processing environment that must be countered by system design.

In October **1997,** a computer security response **team,** representing the **MAISRC,** assembled a team of Component and CDA security subject matter experts to conduct a Facilitated Risk Analysis, which identified major and minor risks to the modem DCPDS. Based upon the Facilitated Risk Analysis. the modem DCPDS APM is developing a Risk Assessment Action Plan that will identify what actions will be taken to mitigate the risks and when the necessary actions will be taken.

Final Repo
Reference

Page 9

Comprehensive DCPDS Certification and Accreditation Planning (page 10). We offer clarification and updates regarding the modem DCPDS functional organization actions with respect to modem DCPDS information assurance planning.

1. "The DCPDS functional and acquisition program managers did not develop a comprehensive certification and accreditation plan to protect DCPDS."

Response: Concur with comment.

This statement is technically accurate even though it implies a deficiency which does not exist. CPMS is in compliance with DoD Directive 5200.28, Security Regulations for Automated Information Systems (AIS), dated March 21.1988, which requires a Certification and Accreditation (C&A) Plan before a new system is deployed to operational test and evaluation sites. CPMS is currently preparing a modem DCPDS C&A Plan that identifies the process that will be followed to obtain accreditation of the modem DPCDS. The modem DCPDS C&A Plan will describe the objectives, responsibilities, schedule, technical monitoring, and other activities in support of the C&A process.

2. "On August 21, 1995, the functional program manager assigned certification and accreditation responsibilities to the DPCDS acquisition program manager, creating a potential conflict of interest."

Response: Do not concur.

A conflict of interest does not exist regarding the assignment of certification and accreditation responsibilities. All systems require a Designated Approving Authority (DAA), even those just beginning the acquisition process. For new acquisitions, a "Developmental DAA" would normally be assigned to the developing or lead agency until the system is ready for operations. The CPMS FPM decision to assign the responsibility for the "Developmental DAA" to the modem DCPDS APM was based on published security regulations, including the DoD Directive 5200.28, dated March 21, 1988.

The modem DCPDS APM will not be both the system DAA and certification official. CPMS, in conjunction with the MAISRC, is currently determining which organizational component will serve as the operating modem DCPDS DAA. The operating modem DCPDS DAA will appoint the certification official, oversee the certification and accreditation process, and approve the system based on the level of risk identified. The operating modem DCPDS DAA will be appointed prior to completion of the modem DCPDS C&A Plan. This decision will also be documented in updated revisions of the modern DCPDS Security Policy and Security Support Plan.

Final Report Reference

3. "The DCPDS functional program manager and acquisition program manager did not adequately establish and document in the DCPDS security support plan a system certification plan even though DCPDS is scheduled to begin operations at selected locations within 6 months. The DCPDS program managers recorded security policy and a security support plan, neither of which recorded an agreed-to certification and accreditation process for the DCPDS DAA and the certification offkial."

Response: Concur with comment.

The modem DCPDS Security Policy and Security Support Plan were never intended to fulfill the requirement for the modem DCPDS C&A Plan. However, these are two of the security-related documents that comprise a C&A Plan. The modem DCPDS Security Support Plan provides an overview of the strategy for designing, developing, and implementing information system security for the modem DCPDS and establishes the methodology for validating system security requirements outlined in the modem DCPDS Security Policy. The modem DCPDS Computer Security Working Group (CSWG) has recently completed a review of these program documents.

The CPMS FPM is currently revising the modern DCPDS Security Policy (Enclosure (1)) and the Security Support Plan (Enclosure (2)). CPMS will publish a coordinated modem DCPDS Security Policy and Security Support Plan in December 1997. In compliance with DoD Directive 5200.28, dated March 21, 1988, these documents will more clearly defme the roles and responsibilities for the operating modem DCPDS DAA and certification official in the certification and accreditation process. CPMS will also complete the modem DCPDS C&A Plan before the modem DCPDS is deployed to the operational test and evaluation sites.

Page 11 Revised

DCPDS Commercially Procured Software (page 12). "The DCPDS functional and acquisition program managers recommended a commercial software alternative but did not include information assurance as a criterion for comparison when selecting the software."

Response: Concur.

Computer security was a criterion in the selection of the COTS Human Resource Information System (HRIS) for the development of the modem DCPDS. Three COTS HRIS products were evaluated based on the capability to satisfy the Class C-2 security criteria in accordance with DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria."

The Draft Preliminary Technical Assessment, dated August 21, 1995, described the four assessment criteria used in evaluating each of the COTS HRIS products. The assessment criteria were architecture; data and integration; standards compliance, includingTechnical Architecture for Information Management (TAFIM); and development environment and tools. The Draft Preliminary Technical Assessment, Paragraph 3.3, indicated the security standards that were used in evaluating how well each COTS HRIS product met the assessment criteria for security

Final Repo
Reference

standards compliance. The modem DCPDS APM prepared a Commercial HRIS Vendor Questionnaire for the three COTS HRIS vendors. Each vendor was required to provide information regarding system security features, including how each product directly complies with a C-2 level of trust. Each vendor was also required to describe how each product or supporting products would ensure confidentiality, integrity, and availability of civilian personnel data.

RECOMMENDATIONS FOR CORRECTIVE ACTION (PAGE 16)

Page 17

Deleted

Recommendation 2a: "Revise the operational requirements document to fully comply with DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Program (MDAPs) and Major Automated Information System (MAIS) Acquisition Program," March 15, 1996, to include validated threat information."

Response: Nonconcur.

The ORD identified the functional requirement that the modem DCPDS must satisfy the Class C-2 (i.e., Controlled Access Protection) security rating at the time of initial operating capability. Systems in this class require discretionary access control, making users individually accountable for their actions through log-in procedures, auditing of security-related events, and resource isolation. A computer security response team, representing the MAISRC, assembled a team of Component and CDA security subject matter experts to review security documentation, conduct a Facilitated Risk Analysis, and develop a plan to take the necessary steps to ensure that data are protected in the modem DCPDS. In response to the October 15, 1997 memorandum from the MAISRC Acting Chair, CPMS developed a 30-60-90 day plan of action to address the information assurance for the modem DCPDS. On November 12, 1997, the Acquisition IPT chairs approved the Information Assurance Plan of Action.

DoD Regulation 5000.2-R, change 2, dated October 6, 1997, requires that major defense acquisition programs (ACAT I) reference a Defense Intelligence Agency (DIA)-validated information warfare threat assessment. This regulation also states that "in some non-warfighting systems, the threat may be listed as not applicable." The modem DCPDS is a non-warfighting system. The Facilitated Risk Analysis provided a comprehensive list of threats and is a more appropriate analysis for an administrative system.

Additional information supporting this response can be found in our earlier response to the statement on Owrational Reauiremeots (page 9).

Page 8

Recommendation 2b: "Provide the acquisition program manager with functional requirements of validated threat information and funding for the protection of DoD civilian personnel data."

Revised, Renumbere as Recommen ation 2.a.

Response: Nonconcur.

This is not recognized as a program deficiency. CPMS has provided and will continue to provide the APM any information it has on threats to the system as described in the previous

Final Report Reference

Page 8

Revised, Renumbered as Recommend-ation 2.b.

response to Operational Requirements (page 9), Comarehensive DCPDS Certification and Accreditation Planning (page 10), and DCPDS Commercially Procured Software (page12). Funding is not an issue since the commercial product being used is C-2 compliant.

Recommendation 2c: "In coordination with the acquisition program manager and the designated approving authority, approve a certification and accreditation plan to protect the Defense Civilian Personnel Data System."

Response: Concur with comment.

CPMS is already working on determining which organizational component will serve as the operating modem DCPDS DAA, as described in the response to **Comarehensive DCPDS Certification and Accreditation Planning (page 10).**

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE COMMUNICATIONS AND INFORMATION CENTER
WASHINGTON DC

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

FROM: **AFCIC/SYS**
1250 Air Force Pentagon
Washington DC **20330-1250**

SUBJECT: **DoD IG** Draft Report, Information Assurance of the Defense Civilian Personnel Data System (Project No. **7RE-3006.01**)

The Air Force concurs with the comments provided by the Designated Acquisition Commander (DAC) without addition or change. We will continue to work with you to ensure the necessary security requirements are met. My point of contact is Major **Geoffrey** Gipson **AFCIC/SYSS,** (703) 695-0767.

Walter M. Washabaugh
WALTER M. WASHABAUGH, Col, USAF
Chief, Business Systems Division
Air Force Communications and Information Center

Attachment:
ESC/CC Comments

cc:
ESC/CC
ESC/IO
CPMS (Dr. **McCullar**)
SAF/AQI
AFPC/DPD (Mr Densberger)

Guardians Of The Fifth Dimension

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS ELECTRONIC SYSTEMS CENTER (AFMC)
HANSCOM AIR FORCE BASE MASSACHUSETTS

U.S. AIR FORCE 50 1947 - 1997

DEC 03 1997

MEMORANDUM FOR SAF/AQI

FROM: ESC/CC
9 Eglin St
Hanscom AFB, MA 01731-2109

SUBJECT: Comments on DoD IG Draft Report, Information Assurance of the Defense Civilian Personnel Data System

I have reviewed the subject report (Project No. 7RE-3006.01, dated 30 Oct 97). The attachment contains comments against the draft report and its findings. Recommend you forward *comments to* DoD IG through OSD/C3I. My point of contact is Maj *Cynthia Cox,* DSN 478-8360.

RONALD T. KADISH
Lieutenant General, USAF
Commander

Attachment:
Comments

cc:
AFCIC/SYSS (Maj Gibson)
AFPC/DPD (Mr. Densberger)
ESC/IO

Golden Legacy, Boundless Future... Your Notion's Air Force

Final Repc
Referenc

**Designated Acquisition Commander's Response
to Draft Audit Report on
Information Assurance of the Defense Civilian Personnel Data System,
Project No. 7RE-3006.01,
Dated October 30, 1997**

Section I: Audit Background

Revised

Change "The DCPDS initial operational capability is scheduled for February 1998, and full operational capability is scheduled for June 1999" to "The DCPDS initial operational capability will be tested at selected sites beginning in June 1998. The modern DCPDS is scheduled to begin full-scale deployment in January 1999 and achieve full operational capability by September 1999."

Section II: Draft Audit Report Findings:

Finding: The functional and acquisition program managers did not consider computer security as a criterion to select the commercial software solution to process DCPDS personnel data. (Page 4, 2nd paragraph, 3rd bullet)

Response: Non-concur

a Computer security was a criterion in the selection of the commercial software solution for processing DCPDS personnel data. The source selection Product and Vendor Criteria previously provided to the audit team did not list computer security. However. the Draft Preliminary Technical Assessment, dated August 21, 1995, describes additional assessment criteria used to evaluate each of the commercial products. It includes an assessment of architecture data and integration, standards compliance, including Technical Architecture for Information Management (TAFIM); and development environment and software tools.

b. Each vendor was required to provide information regarding system security features to include how each product directly complies with a C-2 level of trust. Additionally, each vendor was required to describe how their product or supporting products will ensure confidentiality, integrity, and availability of civilian personnel data.

c. Paragraph 3.3 of the Technical Assessment identifies the security standards used to evaluate how well each of the commercial products met the assessment criteria for security standards compliance.

Finding: **The functional and acquisition program managers did not adequately incorporate information assurance recommendations that the subject matter experts provided. (Page 4, 2nd paragraph. 4th bullet)**

Response: Non-concur

a. The acquisition program management security staff has maintained a close relationship with security experts in numerous DoD and Federal organizations and has incorporated many of their suggestions and recommendations. Agency-specific information regarding our coordination with information protection subject matter experts is provided in the following paragraphs.

(1) **National Security Agency (NSA): The** acquisition program management security **staff has** worked with Mr. Gary **Woodward** and Mr. Jack Adams of **NSA's** Defense Messaging System (DMS) program management office regarding the use of DMS' **MISSI Fortezza** technology as a potential method of encrypting DCPDS data. Both NSA and the modem DCPDS Central Design Activity (CDA) saw great potential in using the same technical solution for e-mail and personnel data. Formal briefings and meetings resulted in a decision to develop a joint test effort located at the CDA. Subsequent technical evaluation showed that the DMS **Fortezza** is technically incompatible with the DCPDS client server communications architecture and the related use of SQL Net. The CDA encouraged NSA to develop a **DCPDS-compatible** Fortezza solution. Plans for joint testing are postponed until a DCPDS compatible solution is available. Although NSA has not produced a compatible **Fortezza** asset to date, the invitation for joint testing remains open.

(2) National Institute **of Standards and Technology (NIST): The** acquisition program management security staff has evaluated and continues to evaluate information protection (encryption) products that are in compliance with Federal Information Processing Standards **(FIPS)** Publication 140-I and the Cryptographic Modules Validation List for compatibility with the DCPDS communications architecture. We have also **asked the Air** Force Information Warfare Center to evaluate some suggested encryption products for use with DCPDS. Those that have been identified as compatible with our communications architecture have undergone an economic analysis to determine the economic feasibility of the encryption solution.

(3) **Defense Information** Systems **Agency (DISA): The** acquisition program management security **staff has** had extensive dealings with DISA **officials** over **the** past two years. We have met formally with Mr. David Hughes (DISA Deputy Chief of Staff for Security) and members of his staff regarding information protection solutions for our and similar Oracle-based systems. An important input from Mr. Hughes was that the vast majority (about 80% or better) of threat to **NIPRNet** connectivity data is due to unauthorized intruders obtaining access to the computers, and that the primary defense should focus on securing the data in the computers.

(4) **AF information Warfare Center (AFIWC): The** acquisition program management security staff has enjoyed a long and productive association with **AFIWC** in regards to DCPDS Information Protection solutions. **AFIWC** information

protection experts helped us develop the standard security configuration settings for the servers in the DCPDS client-server environment. These settings are included in the DCPDS Trusted Facility Manual. They provided formal evaluations of encryption products recommended by AFCA/SYS (e.g., AlliedSignal's KIV-7, and Nortel's Entrust). At our request, AFIWC performed an on-line survey against servers located at the CDA. The results were used to improve our security posture. Finally, we entered into an agreement with AFIWC to test a new sub-IP layer, application independent encryption technology, which if successful, will provide a low cost encryption solution for DCPDS and other sensitive but unclassified applications.

b. Since the audit report does not provide any specifics regarding "advice" we assume it deals with the issue of encryption. Protecting DCPDS data with encryption is a very complex issue and is being addressed by the DCPDS Acquisition Oversight Integrated Process Team (IPT) formed by Brig. Gen. Nagy (SAF/AQI) and Dr. Margaret Myers (OASD (C3I)).[1] At the 7 October, 1997 Acquisition IPT, the OASD(C3I) representative indicated the requirements and policy for encryption are extremely gray. For example, DoD Directive 5200.5 states, "Sensitive information subject to the P.L. 100-235 may be protected during transmission, at the discretion of the DoD Component, by products validated by the National Institute of Standards and Technology as meeting the criteria of applicable Federal Information Processing Standards or by NSA-endorsed COMSEC pmducts. techniques, and protected services." DoD should review and clarify/update the "may be protected" statement and publish waiver and deviation guidance. The OASD(C3I) representative went on to say that one of the key problems is the number of interfaces that exist in business systems like DCPDS. Even if DCPDS data were encrypted, the level of security achieved could be lost as the data are shared with other unclassified systems.

Section III Recommendations for Corrective Action

Recommendation: We recommend that the Commander, Electronics Systems Center, Air Force Material Command, direct the acquisition program manager to develop a comprehensive certification and accreditation plan for the Defense Civilian Personnel Data System that: (Page 17, Recommendation 3)

a. Defines computer security measures to minimize the high risks and the magnitude of harm or loss.

Response: Concur

The certification and accreditation plan will describe computer security measures. In addition, the acquisition program management staff is currently preparing an Information Protection document for the DCPDS which defines the computer security measures to minimize the risk to DCPDS data and how the security requirements of

[1] Action Item No. 97-A-4, OSD/C3I will lead the effort to determine if encryption of DCPDS data will be required.

discretionary access control, object reuse, identification and authentication, and audit are to be satisfied ECD: Jan 98.

In addition to the threats identified in the ORD, the DCPDS Modernization Program Initial Risk Assessment, dated 13 December 1995, provided a more in-depth discussion of system threats. As stated in the Executive Summary "The transition of the DCPDS from a relatively closed mainframe environment to an open systems remote access client-server environment, while resulting in significant improvements in functionality and information availability, greatly magnifies security concerns. Vulnerabilities which exist in all computer systems and networks are largely expanded in number and degree. Of the vulnerabilities particular to DCPDS, those attributable to human behavior, technology related and natural disasters, over 80 percent are attributable to human behavior through error, negligence, ignorance, carelessness, lack of experience or malice. While the greatest risks to DCPDS are from the insider, the threat from attackers on the Internet is rapidly expanding; both threats must be addressed for DCPDS."

And lastly, the DCPDS Security Policy Decomposition Matrix, dated January 1996, identified 209 specific security requirements for the protection of the DCPDS data. These requirements were provided to the developers who, in conjunction with the acquisition program management security staff, determined how best to satisfy the security requirements thereby providing protection for the DCPDS data and resources.

b. Includes computer security requirements in contract solicitations or other instruments for the Defense Civilian Personnel Data System to comply with requirements of DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, where applicable.

Response: Concur

There are no further acquisition decisions planned for DCPDS modernization at this time. However, if additional contract solicitations or other instruments must be made, computer security will be considered.

c. Incorporate applicable recommendations made by technical experts on protection needs for DoD civilian personnel data and computer resources used to process those data.

Response: Concur

(1) During the week of October 6, 1997, a representative of the MAISRC security program assembled a team containing representatives from Components and the acquisition program management staff to review security documentation, conduct a Facilitated Risk Analysis, and develop a plan to take the necessary steps to ensure data is protected in the Modem DCPDS system. Following the week-long intense review of DCPDS security, an action plan for Information Assurance was developed by CPMS and subsequently briefed to the Acquisition IPT on 12 November 1997. This plan contains specific taskings and milestone dates.

Final Repc
Referenc

(2) *The* acquisition program management staff will continue to maintain a close liaison with security experts in other DoD and Federal organizations. Recommendations made by these and other activities will continue to be reviewed for applicability, architectural compatibility, and economic feasibility. Increasing component participation in the Computer Security Working Group will provide enhanced peer review of DCPDS policy recommendations and technical proposals made by these organizations. Encryption solutions will continue to be evaluated by a joint test team from the acquisition program management staff and the Air Force Information Warfare Center to determine their technical suitability for implementation in a large client server enterprise environment.

d. Appoints a certification official independent of and acceptable to the Defense Civilian Personnel Data System designated approving authority.

Response: Concur

The functional program management staff will appoint a certification official. **ECD: Jan 98.**

e. The Defense Civilian Personnel Data *System* designated approving authority and the functional system proponent or representative agree to.

Response: Concur

The functional program management staff is currently preparing a certification and accreditation plan that identities the process that will be followed to obtain accreditation of the DCPDS. ECD: Jan 98.

Section IV Material Management Control Wepkness

Finding: Management's self-evaluation did not identify the DCPDS program or the computer security as an assessable unit and, therefore did not identify or report the material management control weakness identified by the audit. However, management did identify concerns for the DCPDS computer security and provided an audit suggestion to the Inspector General, DoD. (Page 22)

Page 21

Response: Concur

An assessable unit called "modernization planning support office" was added to the Five Year Management Plan. The plan was included as part of the FY97 Annual Statement requited under the Federal Mangers' Financial Integrity Act (FMFIA) of 1982. **Action complete.**

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

Thomas F. Gimble
Mary Lu Ugone
Cecelia A. Miggins
Karim Malek