

Audit
Report



INFORMATION ASSURANCE FOR THE DEFENSE
CIVILIAN PERSONNEL DATA SYSTEM -
WASHINGTON HEADQUARTERS SERVICES

Report No. 98-143

June 3, 1998

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, Home Page at: WWW.DODIG.OSD.MIL.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

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

Acronyms

CSU	Customer Support Unit
DCPDS	Defense Civilian Personnel Data System
RSC	Regional Service Center
WHS	Washington Headquarters Services



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

June 3, 1998

MEMORANDUM FOR DIRECTOR, ADMINISTRATION AND MANAGEMENT
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Audit Report on Information Assurance for the Defense Civilian Personnel
Data System - Washington Headquarters Services
(Report No. 98-143)

We are providing this audit report for review and comment. This is the final of four reports on the Defense Civilian Personnel Data System. We considered management comments on a draft of this report in preparing it.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. As a result of management comments, we revised Recommendation 1.c. Accordingly, we request that the Director for Personnel and Security, Washington Headquarters Services, provide comments on Recommendation 1.c., by August 3, 1998.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049) or Ms. Cecelia A. Miggins at (703) 604-9046 (DSN 664-9046). See Appendix F for the report distribution. The audit team members are listed inside the back cover.


Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-143
(Project No. 7RE-3006.03)

June 3, 1998

Information Assurance for the Defense Civilian Personnel Data System - Washington Headquarters Services

Executive Summary

Introduction. This report is the last of four reports in our ongoing review of the Defense Civilian Personnel Data System. The previous reports discussed acquisition management controls for the Defense Civilian Personnel Data System, information assurance controls for the overall system, and information assurance controls for the Defense Civilian Personnel Data System as it related to Navy. The Defense Civilian Personnel Data System currently in operation is a legacy automated information system that processes sensitive-but-unclassified information for at least 750,000 DoD civilian personnel records. The DoD is modernizing the Defense Civilian Personnel Data System as it regionalizes the delivery of civilian personnel service into 22 regional service centers and approximately 300 customer support units. The modern Defense Civilian Personnel Data System is scheduled to replace the legacy system when regionalization is completed. The Washington Headquarters Services, Human Resource Services Center, will serve as one of the three Defense agency regions and serves seven customer support units, processing approximately 10,000 personnel records.

Audit Objectives. The overall audit objective was to evaluate the adequacy of information assurance for the Defense Civilian Personnel Data System at Washington Headquarters Services. Specifically, we evaluated security planning, risk analysis, and security management. We did not evaluate the security of network and communications infrastructure because DoD resources were not available to conduct vulnerability assessments. We also reviewed the management control program as it applied to the audit objectives.

Audit Results. Washington Headquarters Services has a security policy, security plan, contingency plan, and system access and physical security controls in place; however, it needs to improve information assurance for the Defense Civilian Personnel Data System. Without adequate information assurance controls, Washington Headquarters Services cannot ensure the confidentiality, integrity, and availability of more than 10,000 personnel records. See Part I for the complete discussion and Appendix A for details of the review of the management control program.

Corrective Actions Taken or Planned. Washington Headquarters Services initiated the purchase of security software that will work with its recently purchased firewall. Washington Headquarters Services plans to use the security software to manage and

audit all servers on the network and to perform a systems security risk-and-vulnerability assessment. Also, Washington Headquarters Services is incorporating an annual mandatory computer security awareness training course in accordance with the Computer Security Act of 1987.

Summary of Recommendations. We recommend that the Director for Personnel and Security, Washington Headquarters Services, improve the information assurance program by directing the appropriate security personnel to conduct a risk analysis to identify and define overall system threats and vulnerabilities; conduct a systems test and evaluation; and establish a memorandum of agreement with customer support units to complete a security plan, contingency plan, and system accreditation and to conduct a risk analysis, as well as systems test and evaluation. We also recommend that the Technical Director, Directorate of Personnel Data Systems, Air Force Personnel Center, coordinate with Washington Headquarters Services training requirements for designated security personnel for the Defense Civilian Personnel Data System information assurance program.

Management Comments. The Director, Washington Headquarters Services, concurred with all but one recommendation, stating that no command and control relationship exists between the Washington Headquarters Services Regional Service Center and the customer support units. He noted that each customer support unit is responsible for completing its own security plan, security policy, contingency plan, system accreditation, risk analysis, and systems test and evaluation. The Department of the Air Force concurred with the recommendation and initiated needed actions. See Part I for a discussion of management comments and Part III for the complete text of the management comments. Also, see Appendix E for a discussion of management comments on the finding.

Audit Response. The Washington Headquarters Services comments were partially responsive. Despite the lack of a command and control relationship between the Washington Headquarters Services Regional Service Center and the customer support units, risks exist in relation to the confidentiality, integrity, and availability of personnel data processed using the Defense Civilian Personnel Data System. Although each customer support unit is responsible for completing its own security requirements, the customer support units can access the Washington Headquarters Services Regional Service Center regional database. The Washington Headquarters Services Regional Service Center therefore should seek assurance that the customer support units have adequately implemented security within their information technology environments before allowing access to its regional database. A command and control relationship should not be necessary. We request that the Washington Headquarters Services reconsider its position on the revised recommendation to establish a memorandum of agreement with its customer support units and provide further comments by August 3, 1998.

Table of Contents

Executive Summary	i
Part I - Audit Results	
Audit Background	2
Audit Objectives	3
Information Assurance Program	4
Part II - Additional Information	
Appendix A. Audit Process	
Scope and Methodology	18
Management Control Program	19
Appendix B. Summary of Prior Coverage	20
Appendix C. Glossary	24
Appendix D. Configuration for the Defense Civilian Personnel Data System	27
Appendix E. Management Comments on the Finding and Audit Response	28
Appendix F. Report Distribution	31
Part III - Management Comments	
Washington Headquarters Services Comments	34
Department of the Air Force Comments	43
Civilian Personnel Management Service Comments	50

Part I - Audit Results

Audit Background

Defense Civilian Personnel Data System. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) designated the Defense Civilian Personnel Data System (DCPDS) as an interim standard system in an April 22, 1991, memorandum. The memorandum designated the Secretary of the Air Force as the executive agent for the DCPDS. At that time, DCPDS consisted of a core system, the Air-Force-developed Personnel Data System-Civilian, plus distinct Army and Navy versions of Personnel Data System-Civilian. Since 1991, DoD has transitioned the Military Departments and most Defense agencies to a standard DCPDS. The modern DCPDS program will provide a seamless automated information system that will provide support for personnel policy actions and personnel decisions during peacetime, contingencies, and wartime. The modern DCPDS will support all DoD Components worldwide and will be used by personnel officials, employees, managers, and senior leadership at all levels of DoD operations throughout the world. The modern DCPDS is envisioned to enable one personnel specialist to provide personnel services to about 100 civilian personnel. The modern DCPDS is also envisioned to eliminate duplicative DoD Component and Defense agency personnel system costs and to reduce maintenance costs for mainframe computers. The current operational DCPDS supports the Military Departments and Defense agencies and consists of DCPDS software applications called personnel process improvements. The personnel process improvements are an important element in migrating to the modern system. The personnel process improvements application programs provide electronic means to generate, route, and process personnel actions; create and classify positions; initiate, route, and track training requests; and access current personnel database and associated data from other functional areas. The functionality of the personnel process improvement software applications will be included in the modern DCPDS. The DCPDS interim system is designed to improve and enhance personnel staffs during the DoD transition to a downsized workforce.

Washington Headquarters Services. In November 1993, the Secretary of Defense, by Program Decision Memorandum, directed the Defense agencies to consolidate their civilian personnel operations into three regional service centers (RSCs) from FY 1995 through FY 1998. The RSCs will be the repository for regional DCPDS databases and for official personnel files. In establishing the RSCs, economies of scale will be gained by concentrating personnel support functions at one location. Approximately 60 percent of the current personnel operations workload will migrate from agency personnel offices to the RSC. The remaining workload will be completed in the customer service centers that are managed by the agencies. The key element to achieving the expected cost benefits and other efficiencies is the electronic connections among agency managers and supervisors, the customer support units (CSUs), and the RSC, which collectively will service approximately 10,000 employees. In May 1994, the Defense Agencies Planning Team developed a regionalization concept plan

that would create a National Capital Region in the Washington, D.C., Metropolitan Area in FY 1996, with two additional regions to be established in FYs 1997 and 1998, respectively. Washington Headquarters Services (WHS) would manage the RSC and would consolidate portions of the WHS civilian personnel offices, the Uniformed Services University of the Health Sciences, the Defense Information Systems Agency, the Defense Investigative Service, the On-Site Inspection Agency, the Defense Nuclear Agency, and the Joint Staff.

Audit Objectives

The overall audit objective was to evaluate the adequacy of information assurance for the DCPDS at WHS. Specifically, we evaluated the security planning, risk analysis, and security management. We did not evaluate the security of network and communications infrastructure because DoD resources were not available to conduct vulnerability assessments. We also reviewed the management control program as it applied to the audit objectives. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program. Appendix B provides a summary of prior coverage related to the audit objectives.

Information Assurance Program

WHS possesses a security policy, security plan, and contingency plan, and has system access and physical security controls in place. However, WHS needs to improve information assurance for DCPDS because it did not have the required information assurance controls in place to do the following:

- conduct a risk analysis for its organization to identify and define overall system threats and vulnerabilities as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (The Directive);
- complete a systems security test and evaluation; or
- obtain assurance that its CSUs completed a security plan, contingency plan, and system accreditation and conduct a risk analysis and systems test and evaluation.

Additionally, the DCPDS functional and acquisition program managers did not coordinate with WHS to provide training requirements for designated security personnel for the DCPDS information assurance program.

As a result, without those controls, WHS cannot ensure the confidentiality, integrity, and availability of more than 10,000 personnel records.

Requirements for Information Assurance Controls

The DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988. The Directive states that at a minimum, a risk management program should be in place to determine how much protection is required, how much exists, and the most economical way of providing the needed protection. According to the Directive, risk management is the total process of identifying, measuring, and minimizing uncertain events affecting automated information system resources. It includes conducting a risk analysis, cost benefit analysis, safeguard selection and implementation, security test and evaluation, and systems review. A risk analysis examines system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

The Directive also requires a training and awareness program to provide the security needs of all persons accessing the automated information systems. The security training and awareness program must ensure that all persons responsible

for the automated information system or information in the system and all persons who access the automated information system are aware of operational and security-related procedures and risk.

The Computer Security Act of 1987. The Computer Security Act of 1987 requires computer security plans to be developed for all Federal computer systems that contain sensitive information to ensure data integrity, availability, and confidentiality. The Act defines sensitive information as:

. . . any information, the loss, misuse, or authorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy of which individuals are entitled

The Privacy Act of 1974. DoD civilian personnel data are subject to provisions of the Privacy Act of 1974. 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.

Responsibilities for DCPDS Information Assurance

The DCPDS functional and acquisition managers, and WHS and its CSUs, all have shared roles and responsibilities in safeguarding the DCPDS personnel data. The organizations must fulfill their responsibilities to achieve information assurance for DCPDS.

Directorate of Personnel Data Systems Responsibilities. According to the Air Force Personnel Center Pamphlet 38-1, "Organizations and Functions," April 14, 1997, the Directorate of Personnel Data Systems is responsible for establishing, directing, and managing communications-computer systems security policy and procedures covering DCPDS as it extends to all organizational levels of Federal and DoD organizations and civil agencies.

RSC Responsibilities. The WHS RSC maintains its own domain and is responsible for instituting its own security protection mechanisms and procedures as well as for implementing the minimum security requirements needed for systems to be secure in accordance with DoD regulations. To meet minimum security requirements, WHS must accredit its automated information system. An accreditation is the approval to operate in a particular security mode using prescribed safeguards. Part of the accreditation process is performing a risk analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

CSU Responsibilities. The CSU systems architecture consists primarily of a desktop personal computer that processes sensitive-but-unclassified data. To achieve appropriate measures against threat and vulnerabilities, each CSU is responsible for conducting a risk analysis to identify most risks and threats associated with each workstation that processes personnel data.

Existing Controls

Systems Access Controls. DoD Standard 5200.28-STD, "Department of Defense Trusted Computer Security Evaluation Criteria," December 1985, requires that access to the system is not given to individuals lacking proper authority. Systems access controls were in place at WHS and its CSUs. The RSC generates and controls passwords for access to DCPDS and the personnel process improvements suites. All new users must attend training for the personnel process improvements suites before obtaining access to the DCPDS and the personnel process improvements suites. The system administrator determines the level of access granted to new users based on a matrix received from the CSU. The CSU determines whether requested access is appropriate, based on the responsibilities and duties of the user. Password expiration is not automatically required by the system; however, users are encouraged to change their passwords periodically.

Physical Security. The Directive states that, as a minimum security requirement, automated information systems hardware, software, documentation, and all classified and sensitive-but-unclassified data handled by the automated information system must be protected to prevent unauthorized disclosure, destruction, or modification. The Directive also states that software development and related activities must be physically controlled and protected when the software is used for handling classified or sensitive-but-unclassified information. Physical security controls were in place at WHS and its CSUs. Specifically, at WHS, visitors are required to obtain temporary visitor badges upon entry into the WHS RSC building; servers and network components are located in a locked room that is not accessible to unauthorized personnel; and visitors are escorted while in the computer room facilities. Physical security controls at the On-Site Inspection Agency consist of 24-hour security guards at the building's main entrance, card readers at each entrance, and escorting visitors without a security clearance; a badge requirement for authorized personnel for entry after normal work hours; and camera use. Authorized personnel are required to enter their pin numbers into keypads to gain access to the computer room. Physical security controls at the Joint Staff consist of access being limited to those who have the required clearances and access authorization. The barriers include guards, locks, vaults, security containers, closed circuit television cameras, and intrusion detection alarm systems.

Adequacy of the Information Assurance Program for the Defense Civilian Personnel Data System

WHS did not have an adequate information assurance program for DCPDS. Specifically, WHS did not perform a risk analysis and a systems security test and evaluation. It also did not establish an annual mandatory security training and awareness program. The DCPDS interconnectivity, with numerous information systems and use of the Internet to transfer sensitive personnel data, demands an information assurance program to protect the confidentiality, integrity, and availability of data processed. The underlying requirement of an information assurance program for WHS is to provide reasonable assurance that personnel information that DCPDS processes is reliable and properly safeguarded.

An information assurance program should address key issues such as planning, risk management, and accreditation. The program would provide for collecting information on the organization's security position; planning for program implementation; analyzing, quantifying, and countering risks; planning for disaster recovery; implementing tests; compiling accreditation documentation; and accrediting the system, network, or both. Key documents to be developed as a result of performing the tasks should include the security policy and plan, risk assessment, contingency plan, systems test and evaluation, and a signed statement of accreditation by the designated approving authority. The adequacy of the information assurance program is determined based on the completion and implementation of the documents as well as implementation of system access controls, physical security controls, and an adequate security training and awareness program.

Information Assurance Control Documentation

DoD guidance requires that organizations processing sensitive-but-unclassified data establish and implement an information assurance program. An information assurance program consists of developing and implementing documentation such as a security policy, security plan, contingency plan, and systems security test and evaluation, and having a signed statement of accreditation by the designated approving authority. In addition, WHS and its CSUs must have system access controls, physical security controls, and an adequate security training and awareness program in place.

Security Policy. DoD Standard 5200.28-STD, "Department of Defense Trusted Computer Security Evaluation Criteria," December 1985, states that an explicit and well-defined security policy must be enforced so that no one can access the system without the proper authority. It requires security policy to reflect the laws, regulations, and general policies from which it is derived. WHS and its CSUs developed and implemented security policies for its organizations.

Information Assurance Program

Security Plan. The Computer Security Act of 1987 requires computer security plans to be developed for all Federal computer systems that contain sensitive information to ensure their integrity, availability, and confidentiality. The security plan describes the strategy for implementing information assurance and establishes a methodology for validating the security requirements identified in the security policy. Both WHS and the Joint Staff developed a security plan that establishes a formal security policy and defines the organizational mechanisms necessary for implementation and enforcement. Although the On-Site Inspection Agency's security policy stated that a system security plan will be prepared and maintained for all automated information systems, including networks processing classified or sensitive-but-unclassified information, it did not provide a completed security plan. Without an established security plan, the On-Site Inspection Agency has no assurance that it has developed a strategy for implementing information assurance controls and a methodology for validating security requirements.

Contingency Plan. The Directive requires that contingency plans be developed and tested to ensure that automated information system security controls function reliably and, if they do not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. The Directive also states that if data are modified or destroyed, recovery procedures must be in place. WHS developed a Disaster Recovery Plan, which is a contingency plan outlining the procedures for recovering the primary RSC functions from disruption of services. The primary RSC functions include providing regional database access to the CSUs and the personnel specialists, providing capability for updating the regional database from the DCPDS located at Randolph Air Force Base, and providing RSC employees access to the RSC Administration Servers. The purpose of the Disaster Recovery Plan is to minimize the number of decisions that must be made following a disruption of service. The plan is divided into two sections: the Continuity of Operations Plan and the Emergency Procedures Plan. The Continuity of Operations Plan addresses procedures that must be followed when extended systems outages occur. It also outlines a plan of action to recover from the loss of communications capabilities to network and power outages and hardware failures of the RSC equipment. The Emergency Procedures Plan provides guidance to the RSC System Administrators on the procedures necessary for the system to be shut down and brought back on line safely.

The Joint Staff and the On-Site Inspection Agency did not provide contingency plans. According to the Joint Staff, the development of a contingency plan is based on each organization's determination of whether the applications on its network are critical. According to the Joint Staff, Chief of Security Division, DCPDS is considered critical, and the Joint Staff should have addressed procedures for recovery from disruption of services. According to the On-Site

Inspection Agency, a formal contingency plan is not required for its automated information systems. As a result, the two CSUs have no assurance that they can recover from a disaster or an interruption of services.

Risk Analysis

Requirement for Risk Analysis. The Directive requires that sensitive-but-unclassified information be safeguarded to ensure confidentiality, integrity, and availability. It also requires systems, networks, or both to be accredited. An accreditation is an approval to operate in a particular security mode using prescribed safeguards. Performing a risk analysis is part of the accreditation process in which an examination of system assets and vulnerabilities is conducted to establish an expected loss from certain events based on estimated probabilities of occurrence. In addition to developing DoD guidance requiring a risk analysis, the DCPDS Acquisition Program Manager developed guidance for the RSCs on the need to conduct an operational certification. According to the DCPDS Acquisition Program Manager, the operational certification and risk analysis checklists and guidelines were prepared and distributed to all components. They were also included as attachments to a memorandum issued by the DCPDS Acquisition Program Manager. In the Memorandum for Component Project Managers, "Operational Certification-Regional Service Centers/Risk Analysis Status," January 13, 1997, the DCPDS Acquisition Program Manager emphasized that the certification step is an integral part of the process to ensure system integrity and risk analysis continuity. It further states that one of the phases to the DCPDS program security process requires an initial risk analysis or an update of the current analysis.

Performance of Risk Analysis. Despite the DoD Directive requiring a risk analysis and the guidance provided by the DCPDS Acquisition Program Manager, neither the RSC nor its CSUs -- WHS, the Joint Staff, and the On-Site Inspection Agency -- conducted a risk analysis to identify security risks, to determine their magnitude, and to identify areas needing safeguards. In addition, they did not conduct accreditations on their workstations to support DCPDS certification and accreditation. According to the WHS Information Technology Manager, the RSC did not conduct a risk analysis because it did not have the necessary tools to allow it to thoroughly assess and identify all of the risks and vulnerabilities. He further stated that the RSC was currently procuring security software to assist it in conducting a risk analysis. The Information Technology Manager stated that WHS would be in a better position to assess and identify all of its risks and vulnerabilities upon receipt of the security software, which was received in September 1997. WHS stated that failure to obtain the security software products would result in its inability to complete thorough and comprehensive systems security risk-and-vulnerability assessments, as well as to measure and monitor compliance with its information systems security policies. While major reliance is being placed on the acquisition of security software needed to conduct a risk analysis, it does not release WHS from its responsibility to complete a risk analysis. WHS can use

Information Assurance Program

other alternatives to assess its systems security risks and vulnerabilities. Because WHS has not performed a risk analysis, it does not know what its risks and vulnerabilities are, and it does not have assurance that its system is secure in accordance with DoD regulations. As a result, WHS can not ensure the confidentiality, integrity, and availability of more than 10,000 personnel records.

Followup With WHS by the Directorate of Personnel Data Systems.

Despite the DCPDS Acquisition Program Manager's emphasis on the high priority that effective risk management and security safeguards have with program management, and the need for components' continued support to achieve appropriate measures against threats and vulnerabilities, he did not assess whether the regions performed the operational certifications or risk analyses. The Acquisition Program Manager also did not followup with WHS to determine the status of completion or target completion dates. Specifically, the Central Design Activity Security Coordinator could not provide evidence of a completed operational certification and risk analysis for WHS, or a target date for completion.

Other Information Assurance Controls

Systems Security Test and Evaluation. WHS and its CSUs provided no evidence that they conducted a test and evaluation of the security of the system. The objective of the systems security test and evaluation is to assess the technical and nontechnical implementation of the security design and to ascertain that security features affecting confidentiality, integrity, and availability have been implemented. Systems should be subject to a systems security test and evaluation to ensure that they meet the environmental and operational security requirements.

Accreditation. The Directive requires that each automated information system be accredited to operate in accordance with a designated approving authority-approved set of security safeguards. As of late August, neither WHS nor the On-Site Inspection Agency had an interim accreditation; however, in October 1997, WHS requested and received an extended interim authority to operate. According to the designated approving authority for WHS, WHS was operating without an interim authority from August 7, 1997, through October 6, 1997. In the absence of a signed statement of accreditation, an interim authority to operate should be obtained. (An interim authority to operate can be obtained in 90-day increments up to 1 year.) WHS is currently using the interim system that should be accredited by the designated approving authority to indicate that due care has been taken to protect the information in the system. A reaccreditation will be required when the target system is operational if changes to the interim system will affect the accredited safeguards or the prescribed security requirements. As a result, WHS has no assurance that its CSU systems

are approved to operate using a prescribed set of safeguards at an acceptable level of risk and that CSUs have taken due care to protect the information in the system.

General Information Assurance Training and Awareness. The Directive states that, as a minimum security requirement, a training and awareness program must be in place for the security needs of all persons accessing the automated information system. The security training and awareness program should ensure that all persons responsible for the automated information system or information in it and all persons who access the automated information system are aware of operational and security related procedures and risk. Although security awareness briefings for new users were conducted, security management personnel and users of the DCPDS at WHS have not received periodic annual training in computer security awareness, and an information assurance training and awareness program with annual refresher classes was not implemented. Until recently, management did not emphasize the importance of information systems security training and awareness. According to the Information Systems Security Officer, an annual training program in computer security awareness had not been developed because of other higher priority job assignments and insufficient time available for developing such a program. For example, until recently, the routine job responsibilities of the Information Systems Security Officer included writing contract statements of work, meeting daily with the contractors, preparing information technology budget submissions, attending the information technology budget meetings and briefings, maintaining and continuously updating the inventory database, acting as the network manager, and performing additional duties as assigned. One of the additional duties assigned was the appointment as Information Systems Security Officer that, because it was assigned as an additional duty, did not get the attention needed to implement it as an adequate information assurance training and awareness program. As a result, WHS has no assurance that security management personnel and users have the computer security awareness necessary to promote a secure system environment. According to the General Services Administration Interagency Training Center, lack of awareness is one of the major causes of damage to Federal Government computer operations. The lack of awareness of computer users concerning the types of threats that can cause damage, and the vulnerabilities that permit them to cause damage, is the primary problem. Awareness and planned responses to abnormal events can dramatically reduce the incidence of all other problems.

Coordination With DoD Components on Training Requirements

The DCPDS functional and acquisition program managers did not coordinate with WHS in regard to providing training requirements for designated security personnel, such as the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the System Administrator for the DCPDS. The Information Systems Security Officer, the Network Administrator, and the System Administrators at WHS were not

Information Assurance Program

adequately trained to perform their duties. For example, event audit logs were rarely used because the Network Administrator was not trained on how to use them without an overload of information that would eventually shut down the system. The lack of coordination with WHS and lack of training requirements addressing system-specific responsibilities for security personnel could compromise the security position of the RSCs and CSUs processing personnel data. As a result, required information assurance controls were not in place. Without those controls, WHS can not ensure the confidentiality, integrity, and availability of more than 10,000 personnel records.

Corrective Actions Taken or Planned

In September 1997, in an effort to comply with all aspects of the required security laws, WHS obtained security software that will work with its recently purchased firewall. The security software will be used to manage and audit all servers on the network. Implementing the security tools will allow the WHS information technology managers to establish, manage, and enforce DoD, Office of the Secretary of Defense, and directorate information technology security policies, while providing a framework for integrating systems security functions. The security software will be used to monitor systems security, detect suspicious actions as well as patterns of abuse, and respond automatically according to established security policies. WHS plans to use the security software features to perform a systems security risk-and-vulnerability assessment.

The Information Systems Security Officer at WHS is currently incorporating an annual mandatory computer security awareness training course. The course will be conducted at least annually, in accordance with the Computer Security Act of 1987, and will highlight and summarize the contents of the automated information system security plan. Also, WHS plans to disseminate monthly bulletins from the National Institute of Standards and Technology that address computer security.

Conclusion

The DCPDS functional and acquisition managers did not coordinate with WHS about providing training requirements for designated security personnel for the DCPDS. Personnel designated as the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the System Administrator neither received nor attended any system-specific information assurance training addressing their roles and responsibilities.

Despite DoD requirements and guidance provided by the DCPDS Acquisition Program Manager, neither WHS RSC nor its CSUs -- WHS, Joint Staff, and the On-Site Inspection Agency -- conducted a risk analysis to identify security risks,

determine their magnitude, and identify areas needing safeguards or accreditations to their workstations to support DCPDS certification and accreditation.

Also, other information assurance controls such as a security plan, a contingency plan, a systems security test and evaluation, and a signed statement of accreditation by the designated approving authority were not always developed, completed, and implemented.

Management Comments on the Finding and Audit Response

The Director, Washington Headquarters Services, and the Department of the Air Force commented on the finding. Although not required to comment, the Director, Civilian Personnel Management Service, also commented on the finding. We revised the finding as necessary. A summary of those comments and our response is in Appendix E. The full text of the comments is in Part III.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. As a result of management comments, we revised draft Recommendation 1.c. to clarify the nature of actions needed to improve the information assurance program for DCPDS.

1. We recommend that the Director for Personnel and Security, Washington Headquarters Services, direct the appropriate security personnel to:

a. conduct a risk analysis for its organization to identify and define overall system threats and vulnerabilities.

Washington Headquarters Services Comments. WHS concurred, stating that a risk analysis for the WHS RSC was conducted on October 1, 1997. A copy was provided to the Audit Team Leader on December 31, 1997, after the draft report was issued.

b. conduct a systems security test and evaluation.

Washington Headquarters Services Comments. WHS concurred, stating that a systems test and evaluation on the WHS RSC information technology infrastructure will be completed by the end of the third quarter FY 1998.

c. **establish a memorandum of agreement with the customer support units that access the regional database. The memorandum of agreement should require the customer support units to complete a security plan, contingency plan, and system accreditation and to conduct a risk analysis and systems test and evaluation.**

Washington Headquarters Services Comments. WHS nonconcurred with the draft report recommendation, stating that no command and control relationship exists between the WHS RSC and the CSUs and that each CSU is responsible for completing its own security plan, security policy, contingency plan, and system accreditation and for conducting a risk analysis and systems test and evaluation. Each CSU is responsible to its designated approving authority for obtaining approval to operate. The introduction of the DCPDS client software into the information technology environment of each CSU should trigger the information technology managers to conduct a new risk analysis and obtain an updated approval from the respective designated approving authority. Because WHS has no relationship with the CSU command structure, other than providing human resource management support, no authority currently exists for WHS to conduct an independent risk analysis of any of its customers' workstations or other information technology components.

Audit Response. The WHS comments are partially responsive. Despite the lack of a command and control relationship between the WHS RSC and the CSUs, risks exist in relation to the integrity, availability, and confidentiality of personnel data processed using the DCPDS, and need to be addressed. Although each CSU is responsible for completing its own security plan, security policy, contingency plan, system accreditation, risk analysis, and systems test and evaluation for its information technology environment, the CSUs can access the WHS RSC regional database, which processes more than 10,000 personnel records. The WHS RSC should seek assurance that the CSUs have adequately implemented security within their information technology environments. We have revised our recommendation to have WHS establish a memorandum of agreement with the CSUs that access the regional database to obtain assurance that the CSUs complete a security plan, contingency plan, and system accreditation and that they conduct a risk analysis and systems test and evaluation. The recommendation is not implying that WHS complete required security documentation or conduct an independent risk analysis for its CSUs. The memorandum of agreement should be used as a tool for obtaining assurance that the CSUs have adequately implemented security and are exemplifying good security practices before fielding new interim system software releases and granting the CSUs access to the regional database. We request that WHS provide comments on the revised recommendation.

2. We recommend that the Technical Director, Directorate of Personnel Data Systems, Air Force Personnel Center, develop and implement procedures to coordinate with Washington Headquarters Services and its

customer support units and other DoD Components on establishing system-specific training requirements for designated security personnel for the Defense Civilian Personnel Data System information assurance program.

Department of the Air Force Comments. The Department of the Air Force concurred, stating that in conjunction with the Civilian Personnel Management Service, the DCPDS acquisition program management, is developing a System Security Annex to the DCPDS Training Support Plan. The Annex will be provided to DoD Components to plan, develop, and execute training strategies for functional and technical personnel involved in the operations of the DCPDS. The Annex will also contain the knowledge, skills, abilities, and training requirements for network security officers and users at all operational levels. The System Security Annex was scheduled to be completed by July 1998. Additionally, starting in May 1998, the DoD Components will be required to brief the status of their risk analysis and operational certifications at DCPDS Computer Security Working Group meetings.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

We conducted an on-site review of information assurance policies, procedures, and practices. We reviewed the information planning documents such as the security policy, security plan, risk analysis, contingency plan, and security test and evaluation dated from August 1991 through November 1997. We determined whether systems access controls, physical security, and security training and awareness programs were developed and implemented. We reviewed user, system, and network administrator security practices. We identified and interviewed key security personnel such as the Information Systems Security Manager, Information Systems Security Officer, System Administrator, Network Administrator, and DCPDS managers. We conducted interviews to determine the level of training provided for DCPDS, personnel process improvements software applications, and information assurance. We did not rely on computer-processed data to accomplish the overall audit objective.

Scope Limitation. We did not evaluate the security of network and communications infrastructure because DoD resources were not available to conduct vulnerability assessments.

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 and Standards. We performed this economy and efficiency audit from June through November 1997 in accordance with auditing standards that the Comptroller General of the United States issued, 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 WHS management controls as they related to the DCPDS information assurance program. Specifically, we reviewed WHS controls for security planning, risk analysis, and security management for DCPDS. We also reviewed management's self-evaluation for those controls.

Adequacy of Management Controls. We identified material management control weaknesses for WHS, as defined by DoD Directive 5010.38. The controls for information assurance were inadequate to ensure the confidentiality, integrity, and availability of the information stored on and processed by DCPDS. The recommendations in this report, if implemented, will improve the controls for protecting DCPDS. A copy of this report will be provided to the senior official responsible for management controls at WHS and the Air Force Personnel Center.

Adequacy of Management's Self-Evaluation. Management 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. Management did not conduct an evaluation for FY 1996. Management did not reevaluate all assessable units to ensure that the management controls are addressed for all risk areas in the Personnel and Security Division after the regionalization efforts in FY 1996, as they planned.

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 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 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 noted that attacks are increasing and damaging and are a threat to national security. The General Accounting Office concluded 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

Report No. 98-127, "Information Assurance of the Defense Civilian Personnel Data System - Navy," April 29, 1998. The audit objective was to evaluate the adequacy of information assurance for DCPDS as it related to the Navy. Specifically, the audit evaluated DCPDS security planning, risk analysis, and security management. The report concludes that the Navy Pacific Region and two of its three human resources offices have made DCPDS information assurance a high priority and have computer security programs in place. However, at the beginning of the audit, its Human Resources Office Marine Corps Base Hawaii Kaneohe Bay did not have a security program in place. As a result of the inadequate information assurance controls at Human Resources Office Marine Corps Base Hawaii Kaneohe Bay, the Navy cannot ensure the

confidentiality, integrity, and availability of more than 209,000 Navy and Marine Corps civilian personnel records. The Human Resources Office Marine Corps Base Hawaii Kaneohe Bay has taken corrective action during the audit by developing a security policy and interim authority to operate and by conducting a system security test and evaluation. It has also appointed key security management positions and established a risk analysis safeguard checklist to identify and define overall system threats and vulnerabilities for the computers that run the Defense Civilian Personnel Data System, and it has initiated ongoing security awareness training in accordance with the Computer Security Act of 1987. The report recommended that the Human Resources Office Marine Corps Base Hawaii Kaneohe Bay improve the adequacy of its Defense Civilian Personnel Data System information assurance program by completing an overall security plan and a contingency plan. The Department of the Navy concurred with the recommendations and has initiated needed actions.

Report No. 98-082, "Information Assurance of the Defense Civilian Personnel Data System," February 23, 1998. The audit objective was to determine the adequacy of the information assurance program for major automated information systems, specifically to evaluate DCPDS security planning, risk analysis, and security management. The report concludes that the DCPDS information assurance program did not have adequate controls in place to safeguard DCPDS data and resources. As a result, DCPDS has high risks for unauthorized system access, intentional and unintentional alteration and destruction of data, and denial of service to authorized users. The report recommended strengthened oversight and management of DCPDS information assurance. Also, the report recommended the establishment of information assurance functional requirements and the implementation of information assurance measures to protect DoD civilian personnel data. The Director, Civilian Personnel Management Service, stated that, by acquiring C-2 compliant system hardware and software, no perceivable threats would be 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 threat requirements and funding to protect the DoD civilian 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. Air Force management and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) management agreed with the report's findings and recommendations.

Appendix B. Summary of Prior Coverage

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 cannot ensure that unauthorized individuals can be prevented from accessing, modifying, or destroying the highly sensitive DoD personnel security information that it administers. The report recommended the Defense Investigative Service 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. The Defense Investigative Service did not agree with the overall characterization of its system security status, but agreed with all recommendations and initiated responsive actions.

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 the security safeguards and practices that protect DoD automated information systems need improvement. 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 report 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 finding and recommendations and, in coordination with the Services, Joint Staff, and Defense agencies, was establishing an integrated management process to extend DoD oversight of information assurance programs and activities to all DoD Components.

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 to identify the current risks of transmitting sensitive-but-unclassified information over the Air Force Internet, as well as emphasizing protection requirements to the designated approving 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 separation-of-duty requirements, maintaining consolidated accreditation databases, 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 Defense Science Board 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 action is needed to defend against possible information warfare attacks against DoD systems that could affect 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 was needlessly complex, cumbersome, and costly. The Joint Security Commission made recommendations to create a new policy structure, enhance security, and lower cost by avoiding duplication and increasing efficiency.

Appendix C. 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," March 21, 1988, and definitions from other guidance authorized by that Directive.

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

Availability. Availability is the timely, reliable access to data and information services for authorized users. (*DoD Directive 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997*)

Certification. Certification is the 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 the person responsible to the designated approving authority for ensuring that security is provided for and implemented throughout the life cycle of an automated information system, beginning with the concept development phase through its design, development, operation, maintenance, and secure disposal. (*DoD Directive 5200.28*)

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

Contingency Planning. Contingency plans are developed and tested in accordance with Office of Management and Budget Circular A-130 to ensure that automated information systems' security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. If data are modified or destroyed, recovery procedures must be in place. (*DoD Directive 5200.28*)

¹ National Security Telecommunications and Information Systems Security Instruction.

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

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

Information Systems Security Manager. The Information Systems Security Manager is the person responsible for implementing the overall security program approved by the designated approving authority. The Information Systems Security Manager focuses on automated information system security and should not participate in the day-to-day operation of the automated information system. *(National Computer Security Center-Technical Guideline-027)*

Information Systems Security Officer. The Information Systems Security Officer is the person responsible to the designated approving authority for ensuring that security is provided for and implemented. Specifically, the Information Systems Security Officer is to:

- maintain a plan for system security improvements and progress toward meeting the accreditation,
- evaluate known vulnerabilities to ascertain whether additional safeguards are needed, and
- ensure that audit trails are reviewed periodically. *(DoD Directive 5200.28)*

Risk Analysis. A risk analysis is an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. *(DoD Directive 5200.28)*

Security Awareness Training. Mandatory periodic security awareness training is required for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information. *(Computer Security Act of 1987, Public Law 100-235)*

Security Mode. The security mode is the description of the conditions under which a system operates, based on the sensitivity of the 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, system-high mode, compartment or partitioned mode, and multilevel mode. *(NSTISSI No. 4009)*

Appendix C. Glossary

Security Test and Evaluation. A security test and evaluation is the examination and analysis of the safeguards required to protect an information technology system, as they have been applied in an operational environment, to determine the security posture of that system. *(NSTISSI No. 4009)*

Threat. A threat is any circumstance or event that has 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. Vulnerability is weakness in an information system or its components (such as system security procedures, hardware design, and management controls) that could be exploited. *(NSTISSI No. 4009)*

Appendix D. Configuration for the Defense Civilian Personnel Data System

DCPDS Database. The WHS civilian personnel records are maintained on the DCPDS database at the Air Force Information Processing Activity located at Randolph Air Force Base in San Antonio, Texas. The DCPDS database contains more than 750,000 civilian personnel records, of which 10,000 are processed by WHS. The CSU accesses the regional database at the RSC, which updates the DCPDS database at Randolph Air Force Base.

DCPDS Connectivity. The DCPDS database is networked to regional data bases, which, in turn, link to CSUs and agency managers and supervisors. The RSC network is a Microsoft Windows NT and UNIX Hewlett Packard network with a Fiber Distribution Data Interface backbone. The RSC maintains the regional database that the CSUs access. A connection of the Fiber Distribution Data Interface Networking Services from the router provides the RSC connectivity to the Office of the Secretary of Defense.

The regional database server provides support for the human resources requirements of the entire WHS region. The CSUs access the regional database server for the human resources information that is contained in the database resident on the server. Connectivity from the RSC to the DCPDS database at Randolph Air Force Base is provided through the Non-Classified Internet Protocol Router Network. The CSUs access the database using the Common Desktop Environment Runtime application program from the CSU workstation computers. The Common Desktop Environment Runtime application program allows the CSU users to run the personnel process improvements application programs directly from the user workstation computers. The personnel process improvements application programs provide electronic means to generate, route, and process personnel actions; create and classify positions; initiate, route, and track training requests; and access current personnel database and associated data from other functional areas. The personnel process improvements applications effectively bypass the CSU server and move all of the functionality of the server onto the workstation computer. Currently, no servers are at the CSUs. WHS does not see the need for servers at the CSUs unless the amount of data being processed increases significantly. However, according to the WHS Information Technology manager, depending on the new technical and architectural designs for the target system, the final decision on whether to place servers at the CSUs will be determined by the Central Design Activity and the Civilian Personnel Management Service.

Appendix E. Management Comments on the Finding and Audit Response

The Director, Washington Headquarters Services; the Air Force; and the Civilian Personnel Management Service provided comments on the finding. For the full text of management comments, see Part III.

Washington Headquarters Services Comments on General Information Assurance Training and Awareness. The Director, WHS, stated that the Directorate for Personnel and Security, WHS, performs initial system security training for new employees upon their entry on duty. WHS also conducts annual refresher training for all of its employees. Adequacy of the training materials is currently under review. WHS plans to have a completely revised information system security training program by the fourth quarter of FY 1998.

Audit Response. According to the Information Systems Security Officer, the computer security training was in the form of a briefing and was provided to new employees only. We were not provided data indicating that computer security training was conducted as an annual refresher to all employees. According to the Information Systems Security Officer, an annual computer security training and awareness course will be required for all employees. During the audit, we were told that the Directorate for Personnel and Security, WHS, was incorporating an annual mandatory computer security awareness course that would be conducted in accordance with the Computer Security Act of 1987. That corrective action was noted in the draft audit report.

Department of the Air Force Comments on Coordination With DoD Components. The Department of the Air Force disagreed with the part of the finding that the DCPDS functional and acquisition program managers did not coordinate with WHS about their respective security management roles and responsibilities for the DCPDS information assurance program.

According to the Department of the Air Force, DCPDS program managers coordinated security management roles and responsibilities with DoD Component project management through working group meetings over the last 3 years. Chaired by DCPDS functional program management office, the working group is used as a forum to develop and coordinate security policy, guidelines, and documentation for the modern DCPDS. Additionally, security management roles and responsibilities for the modern DCPDS are specified in the modern DCPDS Security Support Plan.

The modern DCPDS Computer Security Working Group will develop a security annex for the modern DCPDS Training Support Plan. The annex will identify training requirements for security personnel, including the Information Systems

Appendix E. Management Comments on the Finding and Audit Response

Security Manager, the Information Systems Security Officer, the Network Administrator, and the System Administrator. The security annex will also apply to the interim DCPDS.

Civilian Personnel Management Service Comments on Coordination With DoD Components. The Civilian Personnel Management Service disagreed with the finding and stated that the Air Force Personnel Center had coordinated with the DoD Components concerning security management roles and responsibilities for the interim DCPDS. Specifically, the Air Force Personnel Center provided system administrator training, manuals, and software release announcements to the DoD Components covering practices and procedures for granting access to the interim system. The Civilian Personnel Management Service, as the functional proponent for the DCPDS, also stated that recently it had published a coordinated modern DCPDS policy and security support plan, which define the respective security management roles and responsibilities for the modern DCPDS.

The Civilian Personnel Management Service agreed with the finding in that the DCPDS functional and acquisition program managers did not provide any training requirements for the designated security personnel such as the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the System Administrator for the DCPDS. According to the Civilian Personnel Management Service, training requirements for designated security personnel using the legacy and interim DCPDS were not provided. The modern DCPDS Computer Security Working Group will develop a security annex for the modern DCPDS Training Support Plan. The annex will identify training requirements for security personnel, including the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the System Administrator. The security annex will also apply to the interim DCPDS.

Audit Response. The draft report stated that the DCPDS functional and acquisition program managers did not coordinate with WHS in their respective security management roles and responsibilities for the DCPDS information assurance. The statement was not meant to imply that the Air Force Personnel Center did not coordinate with the DoD Components by providing system administrator training, manuals, and software release announcements to the DoD Components' program. Instead, intent was to emphasize the lack of coordination with DoD Components regarding the establishment of training requirements for designated security personnel. To eliminate confusion, we have revised the finding and clarified the report to emphasize the lack of coordination for training requirements for DoD Components.

Appendix E. Management Comments on the Finding and Audit Response

Department of the Air Force and Civilian Personnel Management Service Comments on the Executive Summary and Audit Background. The Department of the Air Force and the Director, Civilian Personnel Management Service, stated that the language used in those elements of the audit report may confuse readers because it does not distinguish between the legacy DCPDS and the modern DCPDS.

Audit Response. We revised the language used in the executive summary and Audit Background to distinguish between the legacy DCPDS and the modern DCPDS.

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)
Under Secretary of Defense for Personnel and Readiness
 Deputy Assistant Secretary of Defense (Civilian Personnel Policy)
 Director, Civilian Personnel Management Service
Assistant Secretary of Defense (Public Affairs)
Director, Administration and Management
 Director, Washington Headquarters Services
 Director for Personnel and Security
Director, On-Site Inspection Agency
Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

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

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Commander, Air Force Personnel Center
 Technical Director, Directorate of Personnel Data Systems, 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 Governmental Reform and Oversight
House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice,
Committee on Government Reform and Oversight
House Committee on National Security

Part III - Management Comments

Washington Headquarters Services Comments



ADMINISTRATION &
MANAGEMENT

OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950



131 EL 1997

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT
DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Audit Report on Information Assurance for the Defense Civilian Personnel
Data System – Washington Headquarters Services
(Project No. 7RE-3006-03)

Enclosed are the management comments to the subject draft Audit report, as requested in your letter of December 17, 1997. Our comments reflect our concurrence or nonconcurrence with the findings and/or recommendations. Projected completion dates for specific actions have been provided for each finding with which we concur. Where we have nonconcurred with your findings and/or recommendations, specific rationale and proposed alternative actions have been provided.

Issues raised in the draft Audit report which do not directly apply to Washington Headquarters Services have not been addressed. Specifically, no response has been made to program management concerns relating to the DoD Civilian Personnel Management Service or the U.S. Air Force Personnel Center.

I appreciate the opportunity to review and comment on your draft report of the audit and your consideration of my remarks in the publication of your final report. Questions should be directed to Mr. A. L. Papenfus, (703) 697-1703, Ms. Linda Dunleavy, (703) 617-7112 or Mr. John Downey, (703) 617-7113.

D. O. Cooke
Director

Findings:

"WHS possesses a security policy, security plan, and contingency plan and has system access and physical security controls in place. However, WHS needs to improve information assurance for DCPDS because it did not have the required information assurance controls in place to do the following:

- a. conduct a risk analysis for its organization to identify and define overall system threats and vulnerabilities as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs), " March 21, 1988 (The Directive),
- b. complete a systems test and evaluation, or
- c. ensure that its CSUs complete a security plan, contingency plan, and system accreditation and conduct a risk analysis and systems test and evaluation."

WHS Response:

a. Concur – A Risk Analysis for the WHS Regional Service Center (RSC) was conducted 1 October 1997, and a copy provided to Ms. Dorothy Dixon, Audit Team Leader, 31 December 1997. Item complete, no further action required.

b. Concur – A systems test and evaluation on the WHS RSC information technology infrastructure will be completed by the end of the 3rd quarter, FY 98.

c. Nonconcur –

(1) No command and control relationship exists between the WHS RSC and the CSUs. Each CSU is responsible for completing its own security plan, security policy, contingency plan and system accreditation and conduct a risk analysis and systems test and evaluation.

(2) As noted on page 6, in the section of your draft Audit Report outlining "Responsibilities for DCPDS Information Assurance", "CSU Responsibilities. The CSU systems architecture consists primarily of a desktop personal computer that processes sensitive-but-unclassified data. To achieve appropriate measures against threat and vulnerabilities, each CSU is responsible for conducting a risk analysis to identify most risks and threats associated with each workstation that processes personnel data." Each CSU is responsible to their Designated Approving Authority (DAA) for obtaining approval to operate. Introduction of the DCPDS client software into their IT environments should trigger their IT managers to conduct a new risk analysis and obtain an updated approval from their respective DAA. Again, since WHS has no relationship with the CSU command structure, other than in providing human resource management support, there currently exists no authority for WHS to conduct an independent risk analysis of any of its customers' workstations or other IT components.

Revised

Findings:

- a. "WHS did not perform a risk analysis and a systems security test and evaluation.
- b. WHS did not establish an annual mandatory security training and awareness program."

WHS Response:

a. Concur: Although incomplete when the DoDIG conducted their audit, a Risk Analysis has been conducted and was forwarded to Ms. Dorothy Dixon, Audit Team Leader on 31 December 1997. A Systems Security Test and Evaluation will be completed NLT the 3rd quarter, FY 1998.

b. Nonconcur. The Directorate for Personnel and Security, WHS, performs initial system security training for new employees upon their entry on duty. Annual refresher training is also conducted for all WHS DP&S employees. Adequacy of the training materials is currently under review. It is planned by the beginning of the 4th quarter, FY 98, to have a completely revised information system security training program.

With the exception of the WHS CSU, the RSC does not provide general information system security training to CSU employees accessing the DCPDS. As with the division of responsibilities relating to the conduct of risk analyses and accreditations, it is the responsibility of the CSU and other customers' IT organizations to provide information assurance training to users. WHS does provide DCPDS system security awareness education during customer training for use of the Personnel Process Improvement (PPI) suite. Users are reminded to safeguard their passwords and not share their user codes and passwords with others. With the implementation of release 5.2 of the PPIs, users are prompted to change their passwords every 180 days.

- a. "Security Plan" (Page 8 of the Audit Report)

Findings:

... "Although the On-Site Inspection Agency's security policy stated that a system security plan will be prepared and maintained for all automated information systems, including networks processing classified or sensitive-but-unclassified information, it did not provide a completed security plan. Without an established security plan, the On-Site Inspection Agency has no assurance that it has developed a strategy for implementing information assurance controls and a methodology for validating security requirements."

WHS Response:

WHS can neither concur nor nonconcur with this finding. As noted above, no command and control relationship exists between the WHS RSC and the CSUs. Each Customer Support Unit is responsible for completing its own security plan, security policy, contingency plan and system accreditation and conduct a risk analysis and systems test and evaluation for their own IT environments.

As noted on page 5, in the section of your DRAFT Audit Report outlining "Responsibilities for DCPDS Information Assurance", "RSC Responsibilities. The WHS RSC maintains its own domain and is responsible for instituting its own security protection mechanisms and procedures as well as for implementing the minimum security requirements needed for systems to be secure in accordance with DoD regulations. To meet minimum security requirements, WHS must accredit its automated information system. An accreditation is the approval to operate in a particular security mode using prescribed safeguards. Part of the accreditation process is performing a risk analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence." As noted above, a Risk Analysis for the WHS RSC was conducted 1 October 1997. System security plans and policy documents were submitted to the WHS DAA. We have recently been verbally informed that our interim accreditation was made permanent.

As noted on page 6, in the section of your draft Audit Report outlining "Responsibilities for DCPDS Information Assurance", "CSU Responsibilities. The CSU systems architecture consists primarily of a desktop personal computer that processes sensitive-but-unclassified data. To achieve appropriate measures against threat and vulnerabilities, each CSU is responsible for conducting a risk analysis to identify most risks and threats associated with each workstation that processes personnel data."

In conclusion, each CSU is responsible to their DAA for obtaining approval to operate. The fact the DCPDS client software has been introduced into the CSU IT environments should trigger the CSU's IT managers to conduct a new risk analysis and obtain an updated approval from their respective DAA. Since WHS has no relationship with the CSU command structure, other than in providing human resource management support, WHS is in no position to gauge the risks or threats imposed by the introduction of the PPI client software on the CSU IT infrastructure. Additionally, no authority currently exists for WHS to conduct an independent risk analysis of any of its customers' workstations or other IT components. Recommend your office address this issue directly to OSLA.

b. "Contingency Plan" (Page 9 of the Audit Report)

Findings:

"The Joint Staff and the On-Site Inspection Agency did not provide contingency plans."

WHS Response:

WHS can neither concur nor nonconcur with this finding. As noted above, no command and control relationship exists between the WHS RSC and the CSUs. Each CSU is responsible for completing its own security plan, security policy, contingency plan and system accreditation and conduct a risk analysis and systems test and evaluation for their own IT environments.

Performance of Risk Analysis

Findings:

"Despite the DoD directive requiring a risk analysis and the guidance provided by the DCPDS Acquisition Program Manager, neither the RSC nor its CSUs – WHS, the Joint Staff and the On-Site Inspection Agency – conducted a risk analysis to identify security risks, to determine their magnitude, and to identify areas needing safeguards. In addition, they did not conduct accreditations on their workstations to support DCPDS certification and accreditation."

WHS Response:

Partially concur. A Risk Analysis for the WHS RSC was conducted 1 October 1997, and a copy provided to Ms. Dorothy Dixon, Audit Team Leader, 31 December 1997. Additionally, Ms. Dixon was furnished a copy of the Operational Certification letter for the WHS RSC provided by the DCPDS Acquisition Program Manager on 14 November 1997. Item complete, no further action required.

WHS can not concur nor nonconcur with references to risk analyses being conducted for any CSUs other than WHS. (The Risk Analysis and accreditation for the WHS CSU is included with that of the WHS RSC.) However, as it pertains to the other supported Customer Support Units and as noted above, no command and control relationship exists between the WHS RSC and those CSUs. Each CSU is responsible for completing its own security plan, security policy, contingency plan, system accreditation and to conduct a risk analysis and systems test and evaluation for their own IT environments.

Systems Security Test and Evaluation (Page 10 of the Audit Report)

Findings:

"WHS and its CSUs provided no evidence that they conducted a test and evaluation of the security of the system."

WHS Response:

Partially concur. A systems test and evaluation on the WHS RSC and the WHS CSU information technology infrastructure will be completed by the end of the 3rd quarter, FY 98.

As previously stated, WHS can neither concur nor nonconcur with references to risk analyses being conducted for any CSUs other than WHS. (The Risk Analysis and accreditation for the WHS CSU is included with that of the WHS RSC.) However, as it pertains to the other supported CSUs and as noted above, no command and control relationship exists between the WHS RSC and those CSUs. Each CSU is responsible for completing its own security plan, security policy, contingency plan, system accreditation and to conduct a risk analysis and systems test and evaluation for their own IT environments.

Findings:

"As of late August, neither WHS nor the On-Site Inspection Agency had an interim accreditation; however, in October 1997, WHS requested and received an extended interim authority to operate. According to the designated approving authority for WHS, WHS was operating without an interim authority from August 7, 1997, through October 6, 1997. In the absence of a signed statement of accreditation, an interim authority to operate should be obtained....WHS is currently using the interim system that should be accredited by the designated approving authority to indicate that due care has been taken to protect the information in the system. A reaccreditation will be required when the target system is operational if changes to the interim system will affect the accredited safeguards or the prescribed security requirements. As a result, WHS has no assurance that its CSU's system is approved to operate using a prescribed set of safeguards at an acceptable level of risk and that due care has been taken to protect the information in the system."

WHS Response:

Concur with this finding as it relates to WHS. As previously noted, however, final accreditation has been verbally received by the DAA. Further, as indicated above, perceived deficiencies with any CSUs should be addressed to a particular Customer Support Unit.

Findings:

"...Although security awareness briefings for new users were conducted, security management personnel and users of the DCPDS at WHS have not received periodic

Washington Headquarters Services Comments

Final Report
Reference

annual training in computer security awareness, and an information assurance training and awareness program with annual refresher classes was not implemented. Until recently, management did not emphasize the importance of information systems security training and awareness. According to the Information Systems Security Officer, an annual training program in computer security awareness had not been developed because of other higher priority job assignments and insufficient time available for developing such a program. For example, until recently, the routine job responsibilities of the Information Systems Security Officer included writing contract statements of work, meeting daily with the contractors, preparing information technology budget submissions, attending the information technology budget meetings and briefings, maintaining and continuously updating the inventory database, acting as the network manager, and performing additional duties as assigned. One of the additional duties assigned was the appointment as Information Systems Security Officer that, because it was assigned as an additional duty, did not get the attention needed to implement it as an adequate information assurance training and awareness program. As a result, WHS has no assurance that security management personnel and users have the computer security awareness necessary to promote a secure system environment."

WHS Response:

Nonconcur. Although the Information Systems Security Officer has other responsibilities assigned to him, those duties did not preclude his developing and implementing a viable computer security awareness program. As noted in the audit report, security awareness briefings for new users are conducted upon their entrance on duty. Additionally, each employee of the WHS Directorate for Personnel and Security receives an annual update briefing and these briefings are documented by the Information Systems Security Officer.

In addition to initial computer security awareness training being provided to all DP&S employees, WHS personnel also provide security awareness briefings as part of the training provided to new users of the DCPDS PPI suite. User training and security briefings are a prerequisite to receiving valid user logons and passwords to access the PPI suite.

Page 11

Not Applicable to WHS.

Findings:

On June 19, 1997, in an effort to comply with all aspects of the required security laws, the WHS initiated the purchase of security software that will work with its recently purchased firewall. The security software will be used to manage and audit all servers on the network.

WHS Response:

Concur. In September 1997, WHS obtained Omniguard/Enterprise Security Manager (ESM) and Omniguard/Intruder Alert (IA), both from Axent Technologies. ESM has been programmed with the security policies of WHS and is used to conduct periodic audits of all servers in the network to gauge compliance with those policies. Reports are provided by ESM to the Information Systems Security Officer and to senior management in WHS regarding the results of those audits. ESM analyzes for example, user password strengths, password ages, and looks for files on servers which may be accessible to unauthorized persons. It then makes recommendations for changes.

Intruder Alert monitors server activities and, according to rules determined by the Information Systems Security Officer, notifies systems administrators of suspicious activities, deny access to apparently unauthorized persons attempting to logon to those servers and compiles daily reports for the Information Systems Security Officer.

~~Information Systems Security Officer, 22 August 1997, WHS Report.~~

Findings:

"1. We recommend that the Director for Personnel and Security, Washington Headquarters Services, direct the appropriate security personnel at WHS to:

- a. conduct a risk analysis for its organization to identify and define overall system threats and vulnerabilities.
- b. conduct a systems security test and evaluation.
- c. ensure that its customer support units complete a security plan, contingency plan, and system accreditation and conduct a risk analysis and systems test and evaluation.

WHS Response:

- a. Concur – A Risk Analysis for the WHS RSC was conducted 1 October 1997, and a copy provided to Ms. Dorothy Dixon, Audit Team Leader, 31 December 1997. Item complete; no further action required.
- b. Concur – A systems test and evaluation on the WHS RSC information technology infrastructure will be completed by the end of the 3rd quarter, FY 98.
- c. Nonconcur –
 - (1) No command and control relationship exists between the WHS RSC and the CSUs. Each Customer Support Unit is responsible for completing its own security plan, security policy, contingency plan and system accreditation and conduct a risk analysis and systems test and evaluation.

Page 13

Revised

(2) As noted on page 6, in the section of your draft Audit Report outlining "Responsibilities for DCPDS Information Assurance", "CSU Responsibilities. The CSU systems architecture consists primarily of a desktop personal computer that processes sensitive-but-unclassified data. To achieve appropriate measures against threat and vulnerabilities, each CSU is responsible for conducting a risk analysis to identify most risks and threats associated with each workstation that processes personnel data." Each CSU is responsible to their DAA for obtaining approval to operate. The fact the DCPDS client software has been introduced into their IT environments should trigger their IT managers to conduct a new risk analysis and obtain an updated approval from their respective DAA. Since WHS has no relationship with the CSU command structure, other than in providing human resource management support, there currently exists no authority for WHS to conduct an independent risk analysis of any of its customers' workstations or other IT components.

Department of the Air Force Comments



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

5 May 98

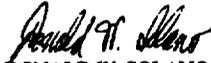
MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

FROM: HQ AFCIC/SYNI
1250 Air Force Pentagon
Washington, DC 20330-1250

SUBJECT: Information Assurance for the Defense Civilian Personnel Data System -
Washington Headquarters Services (Project No. 7RE-3006.03)

This is in reply to your memorandum requesting Air Force comments on the draft subject DoDIG report. The attachment contains AF/DPCX comments to the report findings and recommendations. Please incorporate these comments into the final report. In addition, AFCIC/SYNI and AF/DP have requested SAF/FMPF change the OPR for all DCPDS audit reports to AF/DP. AFCIC/SYNI will remain as the OCR.

If you have any questions or need further assistance please contact Ms. Melinda Palmer, (703)588-6167, AFCIC/SYNI, or Major Mendez, (703)614-2478, AF/DPCX.


DONALD W. SOLANO, Lt Col, USAF
Chief, Information Protection Branch

Attachment:
AF/DPCX response

cc:
AFCIC/ITAI
AFCIC/SYSS
AF/DPCX
SAF/FMPF

Department of the Air Force Comments



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

MEMORANDUM FOR AFCIC/TAI

FROM: AF/DPCX

SUBJECT: DoDIG Draft Report, Information Assurance for the Defense Civilian Personnel Data System- Washington Headquarters Services

27 Apr 98

This is in response to the SAF/FMPF memorandum, 26 March 1998, requesting comments on subject report. The attachment contains the Acquisition Program Management comments against the report findings. Please incorporate the management comments contained in the attachment and forward them to SAF/FMPF.

If you have any questions or need further assistance please contact Maj Mendez, 703-614-2478 or e-mail ruben.mendez@dp.hq.af.mil.

Shirley C. Williams
SHIRLEY C. WILLIAMS
Chief, Plans and Requirements Division
Directorate of Civilian Personnel Policy
and Personnel Plans

Attachment:
Acquisition Program Management Response
cc:
SAF/FMPF
AFCIC/SYSS

**Acquisition Program Manager Management Response
to a Draft Audit Report on
Information Assurance of the Defense Civilian Personnel Data System
Washington Headquarters Services,
Project No. 7RE-3006.03,
Dated December 17, 1997.**

Program Management Comments: One of the circumstances we've encountered during the various Program and Component Information Assurance Audits is that the auditors are viewing procedures and operations of the "interim system," but the findings and comments are directed towards the "modernized" DCPDS, which is still under development. There are significant differences between the two systems. Foremost, the interim system has been operational since 1994 and the modern system will not begin deployment until 1998. The interim DCPDS is the term used to describe applications developed and deployed by program functional experts and Central Design Activity (CDA) analysts and technical experts to support changes in personnel processes resulting from reengineering and/or changes in the structure of personnel services delivery. These applications were originally developed as prototypes but were enhanced and integrated at the request of the DoD Components (Military Services/Federal Agencies) to assist with regionalization of personnel services. Once the modern system is fully deployed, the interim system will be shut down. This interim activity operates within all the requirements and guidelines that apply to the legacy DCPDS and typically received interim accreditation based on mission essential expediency until the modern DCPDS is deployed. The management comments to the report findings are tempered by these distinctive differences. Also, we realize that there is often a time element situation involved with the audit process, specifically the time between the auditor observations and findings and the published report that we are responding to. Several of the following comments are made relative to this situation.

Section I: Draft Audit Report Findings:

Finding: The DCPDS functional and acquisition program managers did not coordinate with WHS about their respective security management roles and responsibilities for the DCPDS information assurance program. (Page 4, 2nd paragraph under the heading of Information Assurance Program)

Response: Non-concur

The program managers have had extensive coordination with WHS project management through a variety of forums and venues concerning security management roles and responsibilities. Executive PM and Component PM meetings have been held monthly for three years. There has been bi-annual or quarterly sessions for at least four years of a Technical Information Group (TIG) with Component management staff participating, covering a variety of

Revised

technical issues, including security. Several special working groups (i.e., Test Planning Working Group, Training Working Group, Computer Security Working Group, System Administration Committee (a TIG special action subgroup)), have been meeting periodically with appointed Component members. Most specific to this finding, the modern DCPDS Computer Security Working Group (CSWG) consists of representatives from the program office, user community, and implementing, operating, and supporting organizations to include Washington Headquarters Services (WHS). This working group, chaired by the functional program management office, is used as a forum for developing and coordinating security policies, guidelines, and documentation for the modern system environment. Security management roles and responsibilities for the modern DCPDS are specified in the modern DCPDS Security Support Plan.
Action Complete.

Finding: Despite the DCPDS acquisition program manager's placing emphasis on the high priority that effective risk management and security safeguards have with program management, and the need for components' continued support to achieve appropriate measures against threats and vulnerabilities, he did not assess whether the regions performed the operational certifications or risk analyses. (Page 10, 1st sentence under Follow-up With WHS by the Directorate of Personnel Data Systems.)

Response: Partially concur

On 13 January 1997, the functional and acquisition program managers jointly issued a memorandum to the Component project managers, subject: DCPDS Modernization Program Operational Certification and Risk Analysis Status of the Regional Service Centers. This package included risk analysis guidelines and a site certification checklist that related to the Personal Process Improvement (PPI) environment and transition to the modern system. The WHS interim system was given interim accreditation by the OSD DAA on 6 October 1997. The regional site certification for WHS was accomplished on 30 October 1997 with all checklist areas, including system security items, rated satisfactory or better. It was specifically noted that this regional setup regarding communications, security, training, etc., was the most outstanding seen to date. But, specifically, as the finding relates to improving overall program management, the status of operational certification and risk analysis for regional site locations will be made an agenda item at all future CSWGs. Components will be required to brief the status of their risk analysis and operational certifications, to include projected milestone dates. Components who are unable to send a representative will be directed to provide the certification and accreditation status in writing for presentation at the CSWG.
Action Complete.

Finding: The acquisition Program Manager also did not followup with WHS to determine the status of completion or target completion dates. Specifically, the Central Design Activity Security Coordinator could not provide evidence of a completed operational certification and risk analysis for WHS, or a target date for completion. (Page 10, 2nd & 3rd sentence under Follow-up With WHS by the Directorate of Personnel Data Systems.)

Response: Concur

Even though the conditions cited in this finding have been resolved (re: time element situation), as mentioned in the previous response, the status of operational certification and risk analysis for regional site locations will be made an agenda item at future CSWGs. Components will be required to brief the status of their risk analysis and operational certification. Components who are unable to send a representative will be directed to provide the certification and accreditation status in writing. This will ensure the CDA Security Coordinator will be able to track the status of all operational certification and risk analysis activities.
Action Complete.

Finding: The DCPDS functional and acquisition program managers did not provide any training requirements for designated security personnel, such as the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the Systems Administrator for the DCPDS. (Page 12, 7th sentence under Coordination With DoD Components)

Response: Concur

a. The PPI software modules are enhancements to the legacy DCPDS environment and operate under the existing regulations and guidelines in place. They streamline many previously manual personnel functions and help offset personnel staff losses resulting from regionalization. In the legacy environment, the participating Components maintained autonomy in many areas to include establishing their own security training requirements based on their respective regulations and directives.

b. A Training Support Plan (TSP) for the modern DCPDS has been developed which will greatly facilitate deployment. It identifies overall training requirements and actions needed to support the development and operational use of the modernized DCPDS. The plan includes training across the spectrum of management, development and corporate-level staff, Regional Support Center (RSC), Customer Support Unit (CSU) and end-user personnel. This plan does not, however, address security in depth. A security annex for the DCPDS TSP will be developed which will identify training requirements for designated security personnel, such as the Information Systems Security Manager, Information Systems Security Officer, Network Administrator, and Systems Administrator for the DCPDS. This annex will be applicable and helpful to the sites still utilizing the PPI environment until they transition to the modern system. ECD July 1998.

Finding: The DCPDS functional and acquisition managers did not provide training requirements for the designated security personnel for the DCPDS. Personnel designated as the Information Systems Security Manager, the Information

Revised
Page 11

Systems Security Officer, the Network Administrator, and the Systems Administrator were neither provided with nor attended any system-specific information assurance training addressing their roles and responsibilities. (Page 13, 2nd and 3rd sentences under Conclusion)

Response: Concur

a. As mentioned in the previous response, those Components who participated in the legacy DCPDS environment maintained autonomy in many areas to include establishing their own security training requirements based on their respective regulations and directives.

b. The Air Force, for example, has developed a two week System Administrators training course targeted at the PPI environment. Air Force Personnel System Managers (PSMs) are scheduled for this course when they are within 6 months of receiving their systems. The acquisition program manager will provide a copy of this training course to the functional program manager for review and then it will be made available to the other Components for possible system wide use.

ECD July 1998

Section II Recommendation for Corrective Action

Recommendation: We recommend that the Technical Director, Directorate of Personnel Data Systems, Air Force Personnel Center, develop and implement procedures to coordinate with the Washington Headquarters Services and its customer support units and other DoD Components on their respective security management roles and responsibilities for the Defense Civilian Personnel Data System information assurance program, including establishing system-specific training requirements: (Page 14, Recommendation 2)

Response: Concur

a. The status of operational certification and risk analysis for regional site locations will be made an agenda item at all future CSWGs. Components will be required to brief the status of their risk analysis and operational certifications, to include projected milestone dates. Components who are unable to send a representative will be directed to provide the certification and accreditation status in writing for presentation at the CSWG.

b. The acquisition program management office will develop a security Annex for the DCPDS TSP. This annex will identify training requirements for designated security personnel, such as the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the Systems Administrator for the DCPDS. This annex will be applicable to the PPI environment.

ECD July 1998.

Section III Material Management Control Weakness

Finding: The controls for information assurance were inadequate to ensure the confidentiality, integrity, and availability of the information stored on and processed by the DCPDS. (Page 17, Adequacy of Management Controls)

Response: n/a
WHS will respond to this finding

Page 19

Finding: Management did not identify the DCPDS program or the computer security as an assembled unit, therefore, did not identify or report the material management control weaknesses identified by the audit. Management did not conduct an evaluation for FY 1996. Management did not reevaluate all assembled units to ensure that the management controls are addressed for all risk areas in the Personnel and Security Division, after the regionalization efforts in FY 1996, as they planned. (Page 17, Adequacy of Management's Self-Evaluation)

Response: n/a
WHS will respond to this finding

Page 19

Civilian Personnel Management Service Comments



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

FEB 13 1998

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

SUBJECT: Proposed Audit Report on Information Assurance for the Defense Civilian Personnel
Data System – Washington Headquarters Services (Project No. 7RE-3006.03)

This memorandum constitutes the functional proponent's response to the Proposed Audit
Report on Information Assurance for the Defense Civilian Personnel Data System – Washington
Headquarters Services dated December 17, 1997 (Project No. 7RE-3006-03). The attached
document responds to the applicable findings, identifies our concerns, and explains the revisions
we believe are necessary so that the final report will accurately reflect Defense Civilian
Personnel Data System program information. We appreciate the opportunity to comment.

Earl T. Payne
Earl T. Payne
Director

Attachment:
As stated

Functional Management Response

**Draft Proposed Audit Report on Information Assurance
for the Defense Civilian Personnel Data System (DCPDS)-
Washington Headquarters Services
DoDIG Project No. 7RE-3006.03**

EXECUTIVE SUMMARY

Introduction (page 1). "This report is the third of four reports in our ongoing review of the Defense Civilian Personnel Data System. The Defense Civilian Personnel Data System is an automated information system that will process sensitive-but-unclassified information for at least 750,000 Defense civilian personnel records at 23 regional personnel servicing centers and approximately 300 customer support units. The Defense agencies will establish four of the 23 regional personnel servicing centers. The Washington Headquarters Services will serve as manager of the National Capitol Region Human Resources Services Center. Initially, the Washington Headquarters Services will process approximately 10,000 personnel records at seven customer support units."

Revised

Response: The proposed language may confuse readers since it does not distinguish between the legacy Defense Civilian Personnel Data System (DCPDS) and the modern DCPDS still under development. To avoid confusion we ask that you substitute the following language:

"This report is the third of four reports in our ongoing review of the Defense Civilian Personnel Data System. The DCPDS currently in operation is a legacy automated information system that processes sensitive-but-unclassified information for approximately 750,000 DoD civilian personnel records. The Department of Defense is modernizing the DCPDS as it regionalizes the delivery of civilian personnel service into 22 Regional Service Centers (RSCs) and approximately 300 Customer Support Units (CSUs). The modern DCPDS is scheduled to replace the legacy system by the time regionalization is completed in FY 1999. The Washington Headquarters Services National Capital Region, Human Resources Service Center (HRSC), will serve as one of the four Defense agency RSCs. The Washington Headquarters Services HRSC serves seven CSUs, processing approximately 10,000 personnel records using the legacy Defense Civilian Personnel Data System."

AUDIT BACKGROUND

Defense Civilian Personnel Data System (page 2). The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) designated the Defense Civilian Personnel Data System (DCPDS) as an interim standard system in an April 22, 1991, memorandum. The memorandum designated the Secretary of the Air Force as the executive agent for the DCPDS. The DCPDS program exists to provide a seamless automated information system that will provide support for personnel policy actions and personnel decisions during peacetime, contingencies, and wartime. The DCPDS will support all DoD Components worldwide and will be used by personnel officials, employees, managers, and senior leadership at all levels of DoD operations throughout the world. DCPDS is envisioned to enable one

Revised

Civilian Personnel Management Service Comments

personnel specialist to provide personnel services to about 100 civilian personnel. DCPDS is also envisioned to eliminate duplicative DoD Component and Defense agency personnel system costs and to reduce maintenance costs for mainframe computers. The current operational DCPDS supports the Military Department and Defense agencies and consists of DCPDS software applications called personnel process improvements. The personnel process improvements are an important element in migrating to the modern system. The personnel process improvements application programs provide electronic means to generate, route, and process personnel actions; create and classify positions; initiate, route, and track training requests; and access current personnel database and associated data from other functional areas. The DCPDS interim system is designed to improve and enhance personnel staffs during the DoD transition to a downsized workforce.

Response: The proposed language may confuse readers since it does not distinguish between the legacy DCPDS and the modern DCPDS still under development. To avoid confusion we ask that you substitute the following language which describes the transition of the legacy DCPDS since it was designated as an interim standard system and clarifies the distinction between the legacy DCPDS and the modern DCPDS.

"The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) designated the DCPDS as an interim standard system in an April 22, 1991, memorandum. The memorandum designated the Secretary of the Air Force as the executive agent for the DCPDS. At that time, DCPDS consisted of a core system, the Air Force-developed Personnel Data System-Civilian (PDSC), plus distinct Army and Navy versions of PDSC. Since 1991, the Department has transitioned the Military Departments and most Defense agencies to a standard DCPDS.

To support the regionalization of civilian personnel service delivery, the Department developed a suite of software applications called Personnel Process Improvements (PPIs) that operate in conjunction with data from DCPDS in a client-server environment. The PPI Suite provides an electronic means to generate, route, and process personnel actions; create and classify positions; initiate, route, and track training requests; and access the personnel database and associated data from other functional areas. The client-server configuration is referred to as the interim DCPDS. The interim system is generally deployed when a Regional Service Center becomes operational.

The Department is now in the process of developing a modern DCPDS. The functionality of the PPI Suite will be included in the modern DCPDS. The modern DCPDS will provide a seamless automated information system that will support personnel policy actions and personnel decisions during peacetime, contingencies, and wartime. The modern DCPDS will support Components worldwide. Personnel officials, employees, managers, and senior leadership at all levels of the Department will use it. The modern DCPDS will also eliminate the need for duplicative Component headquarters personnel systems reduce maintenance costs for mainframe computers."

Information Assurance Program (page 4, 12 and 13). "Additionally, the DCPDS functional and acquisition program managers did not coordinate with WHS about their respective security management roles and responsibilities for the DCPDS information assurance program."

Response: Non concur.

The legacy DCPDS was designed, developed, and implemented as an Air Force personnel system in the mid 1970s. When the ASD (C3I) designated the legacy DCPDS as the interim standard system in 1991, the functional program managers left the existing security management roles, responsibilities, and processes in place.

AFPC has coordinated with the Components concerning the security management roles and responsibilities for the interim DCPDS. AFPC also provided system administrator training and manuals to the Components that cover practices and procedures for granting access to the interim system. On February 12, 1997, AFPC provided Component systems administrators a software release announcement for PPI Version 4.4 of the interim system. This release implemented the first scripts to configure servers and workstations in accordance with the established security policy. AFPC provided another release announcement for the PPI Version 5.0 in June 1997. This announcement described the scripts and actions required to operate the system audit log feature.

CPMS, as the functional proponent for the DCPDS Modernization Program, is responsible for insuring controls are in place to safeguard civilian personnel records in the modern DCPDS. Recently, CPMS published a coordinated modern DCPDS policy and security support plan. These documents clearly define the respective security management roles and responsibilities for the modern DCPDS. In addition, CPMS is in the final process of identifying the organizational component, which will serve as the modern DCPDS Designated Approving Authority (DAA). The modern DCPDS DAA will appoint a certification official who will oversee the Certification and Accreditation (C&A) process, and approve the level of risk for the modern DCPDS. The modern DCPDS DAA will oversee the development of the C&A package. The C&A package will describe the objectives, responsibilities, schedule, technical monitoring, and other activities in support of the C&A process.

Coordination With DoD Components (page 12 and 13). "Specifically, the DCPDS functional and acquisition program managers did not provide any training requirements for designated security personnel such as the Information Systems Security Manager, the Information Systems Security Officer, the Network Administrator, and the Systems Administrator for the DCPDS."

Response: Concur.

The legacy and interim DCPDS operate under existing computer security program regulations and guidelines. CPMS has not provided training requirements for designated security personnel using the legacy and interim DCPDS. In this environment, Components are responsible for establishing their own security training requirements based on their specific regulations and directives.

Pages 4,
11, & 12

Pages 11 &
12

Civilian Personnel Management Service Comments

The modern DCPDS Computer Security Working Group (CSWG), chaired by CPMS, will develop a security annex for the modern DCPDS Training Support Plan. The annex will identify training requirements for security personnel, including the Information Systems Manager, the Information Systems Security Officer, the Network Administrator, and the Systems Administrator for the modern DCPDS.

Under the Regionalization Program, the modern DCPDS will operate in a standard operating environment of servers, workstations, peripherals, and communications networks for civilian personnel operations throughout DoD. A relational database will link to the client-server network located at Regional Service Centers and Customer Support Units. The interim DCPDS is currently deployed in this operating environment. Therefore, the DCPDS Training Support Plan Security Annex will apply to the interim DCPDS.

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
Dorothy L. Dixon
Kathleen Fitzpatrick
Michael T. Carlson
Bernice M. Lewis

