

Audit

Report



INFORMATION ASSURANCE OF THE DEFENSE CIVILIAN
PERSONNEL DATA SYSTEM - NAVY

Report Number 98-127

April 29 1998

Office of the Inspector General
Department of Defense

Additional Information and Copies

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

Suggestions for 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

DCPDS
HRO

Defense Civilian Personnel Data System
Human Resources Office



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

April 29, 1998

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (FINANCIAL
MANAGEMENT AND COMPTROLLER)
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Audit Report on Information Assurance of the Defense Civilian Personnel
Data System - Navy (Report No. 98-127)

We are providing this audit report for your information and use. This is the third of four reports on the Defense Civilian Personnel Data System by the Office of Inspector General, DoD. We considered management comments on a draft of this report in preparing the final report.

Management comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone, Audit Program Director, at (703) 604-9049 (DSN 664-9049); Ms. Cecelia A. Miggins, Audit Project Manager, at (703) 604-9046 (DSN 664-9046); or Ms. Kathleen Fitzpatrick, Audit Team Leader, at (703) 604-8974 (DSN) 664-8974. See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-127
(Project No. 7RE-3006.02)

April 29, 1998

Information Assurance of the Defense Civilian Personnel Data System - Navy

Executive Summary

Introduction. This report is the third of four reports in our ongoing review of the Defense Civilian Personnel Data System. The first report discussed acquisition management controls for the Defense Civilian Personnel Data System and the second report discussed the information assurance controls for the overall system. The Defense Civilian Personnel Data System is an automated information system that will process sensitive-but-unclassified personnel information for 209,000 Navy and Marine Corps civilian personnel records at 8 regional personnel centers and approximately 100 customer support units.

Audit Objectives. The overall audit objective was to evaluate the adequacy of information assurance for the Defense Civilian Personnel Data System as it relates to the Navy. 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. Appendix A discusses the audit process. Appendix B provides a summary of prior coverage related to the audit objectives.

Audit Results. The Navy Pacific Region and two of its three human resources offices have made Defense Civilian Personnel Data System 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. See Part I for the complete discussion and Appendix A for details on the management control program.

Corrective Actions Taken or Planned. 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.

Summary of Recommendations. We recommend 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.

Management Comments. The Department of the Navy concurred with the recommendations and has initiated needed actions. See Part I for a discussion of management comments and Part III for the complete text of the management comments.

Table of Contents

Executive Summary	i
Part I - Audit Results	
Audit Background	2
Audit Objectives	4
Information Assurance Program	5
Part II - Additional Information	
Appendix A. Audit Process	
Scope and Methodology	14
Management Control Program Review	15
Appendix B. Summary of Prior Coverage	16
Appendix C. Glossary	20
Appendix D. Report Distribution	23
Part III - Management Comments	
Department of the Navy Comments	26
Civilian Personnel Management Service Comments	28

Part I - Audit Results

Audit Background

Defense Civilian Personnel Data System. The modern Defense Civilian Personnel Data System (DCPDS) will provide a seamless automated information system for civilian personnel policy actions and personnel decisions during peacetime, contingencies, and wartime. The modern DCPDS will support Military Departments and Defense agencies worldwide and will be used by personnel officials, employees, managers, and senior leadership at all levels of DoD operations. The current operational DCPDS is an interim system designed to improve and enhance personnel staffs during the DoD transition to the modern DCPDS. The interim DCPDS, which this report refers to as DCPDS, resides on a mainframe computer and has separate databases at Military Department or Defense agency levels to support civilian personnel operations. The DCPDS databases are maintained at the Defense Information Systems Agency Defense Megacenter, located at Kelly Air Force Base, San Antonio, Texas. The DCPDS stores, processes, and transmits data for 750,000 personnel records, of which 209,000 belong to the Navy and Marine Corps and are subject to the Privacy Act of 1974 and the Freedom of Information Act. For security purposes, the DCPDS data are labeled "sensitive-but-unclassified."

The DCPDS Acquisition Program Manager has been delegated responsibility for the overall protection of the DCPDS information and the computer resources. The responsibility for the confidentiality, integrity, and availability of the DCPDS information resides with all DoD organizations and persons who have access to the records.

The Navy Regions. The modern DCPDS will enable the Military Departments and the Defense agencies to process, store, and transmit civilian personnel records on databases at 22 regional service centers. Regionalization of civilian personnel operations began in FY 1995. The Navy is consolidating hundreds of full-service Navy and Marine Corps personnel offices into eight regions called human resources service centers¹. In October 1996, the Navy established the Pacific Region, Honolulu, Hawaii.

A region is the repository for official personnel files and regional DCPDS databases. A Navy region maintains a regional database containing personnel records of serviced employees, and the regional database updates the Navy DCPDS database in San Antonio, Texas. The personnel data are transmitted using the Internet. Additionally, the Navy DCPDS database feeds data to other DoD databases; for example, it feeds them to the Defense Civilian Payroll System and the Navy Headquarters System.

¹Regions are called human resources service centers by the Navy and regional service centers by DoD.

A region's mission is to provide information management and processing support for position classification, personnel recruitment and staffing, workforce development, employee benefits and services, and related records management. The Navy and the Marine Corps will reestablish the remaining portions of their civilian personnel offices as independently operated human resources offices² (HROs) focusing primarily on personnel program planning and oversight, policy analysis and development, and management advice and consultation for personnel management within their respective commands. Under the regionalization concept, HROs will support a customer service environment and provide advisory services. In October 1996, three HROs became operational in the Pacific Region at the following locations:

- Pearl Harbor Naval Shipyard, Hawaii;
- Commander Naval Base Pearl Harbor, Hawaii; and
- Marine Corps Base Hawaii Kaneohe Bay, Hawaii.

Safeguarding Personnel Data. DoD civilian personnel data are subject to provisions of the Privacy Act of 1974 and the Freedom of Information Act. The Privacy Act of 1974 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 of 1974 also requires each agency to account for disclosures of information to other organizations and individuals. The Freedom of Information Act requires agencies to make information available to the public but excludes from that disclosure personnel information that would constitute an invasion of privacy. The DCPDS for the Navy must meet provisions of the Privacy Act of 1974 to safeguard the personnel data.

The policy and procedures for safeguarding sensitive-but-unclassified DoD information are prescribed in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988. "Information assurance" and "computer security," as used in this report, are intended to be synonymous. Please see Appendix C for a glossary of terms used in this report.

²Support units are called human resources offices by the Navy and customer support units by DoD.

Audit Objectives

The overall audit objective was to evaluate the adequacy of information assurance of DCPDS for the Navy. 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 adequacy of the DCPDS management control program as it applied to the overall audit objective. 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

The Navy Pacific Region and two of its three HROs possess a security policy, security plan, contingency plan, and interim authority to operate. They also conduct system security test and evaluations, risk analyses, and security training and awareness programs; appoint key security management positions; and have system access controls and physical security controls in place. However, at the beginning of the audit, its HRO Marine Corps Base Hawaii Kaneohe Bay did not have a security program in place. During the audit, the HRO Marine Corps Base Hawaii Kaneohe Bay developed a security policy and an interim authority to operate, conducted a system security test and evaluation and a security training and awareness program, appointed key security management positions, and conducted a risk analysis 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. However, information assurance for the HRO Marine Corps Base Hawaii Kaneohe Bay still needs improvement because it does not have an overall security plan and a contingency plan.

Further, the DCPDS functional and acquisition managers did not coordinate with the Navy about their respective security management roles and responsibilities for the DCPDS information assurance program.

As a result, without those controls, the Navy cannot ensure the confidentiality, integrity, and availability of more than 209,000 Navy and Marine Corps civilian personnel records³ that are processed on the DCPDS.

Requirements for Information Assurance Controls

Federal Guidance. Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1997, recognizes the need for special management attention for security of automated information systems because of the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of management information. In addition, Circular A-130 requires agencies to recognize that, in Federal Government information systems involving personal information, the individual's right to privacy must be protected.

³The Navy Pacific Region maintains a database containing more than 9,000 records. The database links to and updates the DCPDS Navy database, which could allow for possible access to more than 209,000 records if it lacks information assurance controls.

Information Assurance Program

Circular A-130 directs all Federal agencies to protect information commensurate with the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of such information. Circular A-130 requires agencies to incorporate minimum controls for all Government automated information system security programs to include the following:

Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and information process supported by the application and in the management, personnel, operational and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

DoD civilian personnel data are subject to provisions of the Privacy Act of 1974 (the Privacy Act). The Privacy Act generally requires Federal agencies to safeguard personal information from disclosure to any other organization or individual without the consent of the individual to whom the information pertains. The Privacy Act also requires each agency to account for disclosures of information to other organizations and individuals.

The Computer Security Act of 1987 requires that Federal agencies develop computer security plans for all Federal computer systems that contain sensitive information to assure their integrity, availability, or confidentiality. Sensitive information as defined by the Computer Security Act of 1987 is:

. . . 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

DoD Security Requirements. DoD Directive 5200.28 incorporates the provisions of Circular A-130 and provides mandatory minimum automated information system security requirements for systems that process sensitive-but-unclassified information. DoD Directive 5200.28 states that, as 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 DoD Directive 5200.28, 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 identifies threats and vulnerabilities and categorizes the level of risk associated with each.

Existing Controls

The Navy Pacific Region, HRO Pearl Harbor Naval Shipyard, and HRO Commander Naval Base Pearl Harbor have made DCPDS information assurance a high priority and have security programs in place. The offices have performed a computer security accreditation and conducted a risk analysis to identify security risks. As of July 1997, the HRO Pearl Harbor Naval Shipyard and HRO Commander Naval Base Pearl Harbor submitted computer security accreditation packages to the base Information System Security Officer and are waiting for the designated approving authority to accredit the DCPDS computer resources.

Specifically, the sites possess security policy and plans; have system access controls and physical security controls in place; and have performed a computer security accreditation, which included the following:

- contingency plan,
- security test and evaluation,
- risk analysis safeguard checklist,
- security awareness training,
- appointment of key security management positions, and
- interim authority to operate on the local area network.

See Appendix C for a glossary of terms.

Corrective Action Taken. The HRO Marine Corps Base Hawaii Kaneohe Bay has taken corrective action since the start of the audit by performing a risk analysis safeguard checklist, system security test and evaluation, computer survey, and security policy for the computers that run DCPDS. The Marine Corps Base Hawaii has an interim authority to operate the DCPDS on the local area network not to exceed 1 year.

Also, the HRO Marine Corps Base Hawaii Kaneohe Bay and the Marine Corps Base Hawaii have initiated ongoing security awareness training.

The HRO Marine Corps Base Hawaii Kaneohe Bay and the Marine Corps Base Hawaii have completed appointment letters for key security management positions. The letters were awaiting signature of the base designated approving authority.

Actions That Still Need To Be Taken. The HRO Marine Corps Base Hawaii Kaneohe Bay still needs to implement a security plan and contingency plan.

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.

Without an established security plan, the HRO Marine Corps Base Hawaii Kaneohe Bay has no assurance that it has developed a strategy for implementing information assurance controls and a methodology for validating security requirements.

Contingency Plan. DoD Directive 5200.28 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. DoD Directive 5200.28 also states that recovery procedures must be in place in case data are modified or destroyed. The HRO Marine Corps Base Hawaii Kaneohe Bay did not have a contingency plan. As a result, the HRO Marine Corps Base Hawaii Kaneohe Bay has no assurance that it can recover from a disaster or interruption of services.

Configuration for DCPDS

The Navy DCPDS database is networked to regional databases, which, in turn, are linked to HROs at installations throughout the Navy and the Marine Corps. Users at regions and HROs have a network of personal computers, containing system and application software, to facilitate data communication to interact with each other.

The region maintains application software necessary to perform personnel functions on Hewlett Packard minicomputers. All successfully completed personnel transactions are posted to a regional database, then posted to update the Navy DCPDS database in San Antonio, Texas. The personnel data are transmitted across combinations of local area networks using the Internet Protocol method. Most DoD organizations that use the Internet Protocol method access the DCPDS database using the Not Classified Internet Protocol Router Network.

The personnel data are not encrypted when transmitted back and forth between Navy regional databases and the Navy DCPDS database in Texas, leaving the data vulnerable to unauthorized access. If unauthorized access to a computer occurs, all of the resident information is at risk, and other connected networks are also in jeopardy.

Information Assurance Control Documentation

DoD Directive 5200.28 provides mandatory minimum automated information system security requirements for systems that process sensitive-but-unclassified information. Secretary of the Navy Instruction 5239.2 (Navy Security Program 5239.2), "Department of the Navy Automated Information Systems (AIS) Security Program," November 15, 1989, which implements DoD Directive 5200.28, requires that the appropriate designated approving authority accredit automated information systems, networks, and computer resources based on a certification and risk management process. Automated information systems not accredited may operate on a local area network if the designated approving authority has issued an interim authority to operate for a period not to exceed 1 year.

The HRO Pearl Harbor Naval Shipyard and HRO Commander Naval Base Pearl Harbor, which are base-owned, conducted a site accreditation of the DCPDS computer resources as required by the Navy Security Program 5239.2. The HROs provided to the base-level designated approving authority information needed to determine whether the computers are operating within an acceptable level of risk to be placed on the base local area network.

The HROs submitted accreditation packages to the base Information System Security Officer, who reviewed the packages and submitted them for approval to the designated approving authority. If acceptable, the designated approving authority issues a formal declaration that the DCPDS is approved to operate on the base local area network because it meets a prescribed set of security standards.

Responsibilities for DCPDS Information Assurance

The DCPDS functional and acquisition managers and the Navy Pacific Region and its HROs 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 and computer systems security policy and the procedures covering DCPDS at all levels of Federal and DoD organizations.

Navy Responsibilities. As owner of the personnel data, the Navy is responsible for directing, coordinating, and managing security policy and procedures for Navy and Marine Corps personnel offices using DCPDS. The

Navy is also responsible for coordinating and following up on security issues and concerns between the Navy personnel sites and the Directorate of Personnel Data Systems.

Navy Pacific Region Responsibilities. The Navy Pacific Region 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 in accordance with DoD regulations. To meet minimum security requirements, the Navy Pacific Region 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.

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

Coordination With DoD Components

The DCPDS functional and acquisition project managers did not coordinate with the Navy in their respective security management roles and responsibilities for the DCPDS information assurance program. Specifically, the Directorate of Personnel Data Systems, Air Force Personnel Center, does not have an adequate program in place to coordinate and communicate with DoD Components about their respective security management roles and responsibilities for the DCPDS information assurance program. The Directorate of Personnel Data Systems also has not ensured that DCPDS uses the effective security products and techniques required by Circular A-130. The Directorate of Personnel Data Systems has not provided guidance to DoD Components on safeguards and has not followed up to ensure that the DoD Components have implemented corrective actions to guidance.

The Directorate of Personnel Data Systems issued guidelines to DoD Component project managers for DCPDS sites to complete an operational certification in the memorandum, "Operational Certification-Regional Service Centers/Risk Analysis Status," January 13, 1997 (Operational Certification Memorandum).

The Operational Certification Memorandum states that the operational certification process is an integral part of ensuring system integrity and risk analysis continuity, and that the DCPDS security process requires a risk analysis

or an update of the current one. Checklists for operational certification and risk analysis were included as attachments to the Operational Certification Memorandum.

The Directorate of Personnel Data Systems did not set milestone dates for the completion of the operational certification and risk analysis. The Operational Certification Memorandum guidance was not coordinated with and followed up by the Navy Pacific Region or its HROs. The Directorate of Personnel Data Systems does not have a method in place to determine when and whether sites have completed the operational certification.

Coordination of DCPDS security issues is important to provide consistency among all DoD Components operating DCPDS. The lack of coordination is causing DoD Components to take their own approaches to security; that is, they are independently developing their own measures to deal with DCPDS vulnerabilities.

Corrective Action Taken. Since the audit started, a coordinated DCPDS policy and security support plan was published. The plan defines the respective security management roles and responsibilities for DCPDS.

Corrective Action Being Taken. Civilian Personnel Management Service, in conjunction with the Central Design Activity security staff, 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 April 30, 1998.

Conclusion

The Navy Pacific Region, HRO Pearl Harbor Naval Shipyard, and HRO Commander Naval Base Pearl Harbor have made DCPDS information assurance a high priority and have security programs in place. The HRO Marine Corps Base Hawaii Kaneohe Bay took corrective action during the audit by initiating a DCPDS security program.

The Directorate of Personnel Data Systems developed and provided guidance for the security of DCPDS to DoD Component project managers. The guidance emphasized the priority and importance of effective risk management and security safeguards; however, it did not establish milestone dates for completion or follow-up to determine the status of steps performed. The Directorate of Personnel Data Systems should improve its communication and coordination of guidance issued to ensure the confidentiality, integrity, and availability of Navy and Marine Corps civilian personnel records on DCPDS.

Management Comments on the Finding and Audit Response

The Navy concurred with the finding. Although not required to comment, the Civilian Personnel Management Service provided suggestions on the finding, and we made revisions in consideration of management comments. The full text of the comments is in Part III.

Recommendations and Management Comments

We recommend that the Director, Human Resources Office Marine Corps Base Hawaii Kaneohe Bay:

- 1. Complete an overall security plan for the Defense Civilian Personnel Data System.**
- 2. Complete a contingency plan for the Defense Civilian Personnel Data System.**

Management Comments. The Department of the Navy concurred and is working with the base to develop a security plan and a contingency plan, which will ensure the integrity of the computer systems used to hold personnel data and will include backup security controls and data recovery systems, respectively.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

Scope. We judgmentally selected three Navy locations and one Marine location to evaluate the adequacy of information assurance for DCPDS.

Methodology. We conducted on-site reviews of information assurance policies, procedures, and practices. We reviewed the information planning documents such as security policy, security plans, risk analyses, contingency plans, and security test and evaluations dated from November 1989 through November 1997. We determined whether system 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, and DCPDS managers. We conducted interviews to determine the level of training provided for DCPDS information assurance.

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

Use of Computer-Processed Data. We did not use computer-processed data or statistical sampling procedures to evaluate the adequacy of the DCPDS information assurance.

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

Audit Period and Standards, and Locations. We performed this program audit from June through December 1997 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. Accordingly, we included tests of management controls considered necessary.

Management Control Program Review

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 adequacy of Navy management controls as they relate to the DCPDS information assurance program. Specifically, we reviewed 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 a material management control weakness for the Navy, as defined by DoD Directive 5010.38. The controls in place for information assurance were not adequate to ensure the confidentiality, integrity, and availability of the DCPDS data. The recommendations in this report, if implemented, will improve the controls for protecting DCPDS data. A copy of this report will be provided to the senior official responsible for management controls at the Navy.

Adequacy of Management's Self-Evaluation. The Navy management identified personnel offices as assessable units; however, information assurance was not addressed for DCPDS and, therefore, was not identified or reported as a material weakness.

Appendix B. Summary of Prior Coverage

General Accounting Office

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

GAO Report No. AIMD-96-84 (OSD Case No. 1150), "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," May 22, 1996. The report discusses the General Accounting Office review of the extent to which DoD computers are being attacked, the potential for damage, and the challenges faced in responding to the attacks. The General Accounting Office 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. 98-082, "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.

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

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,

Appendix B. Summary of Prior Coverage

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 continue 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 to emphasize protection requirements to the designated approval authorities. Air Force management officials agreed with the overall audit results and planned responsive actions.

Project No. 93058001, "Review of Personnel Concept III System Security and Equipment Management," April 3, 1995. The audit objective was to determine whether selected security and control procedures were properly implemented in the Personnel Concept III computer system. The report concludes that the Air Force did not implement adequate security access protection for the system and did not properly account for computer equipment. The Air Force Audit Agency recommended implementing 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 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 impact the ability of DoD to carry out its responsibilities. The task force recommended 50 actions ranging from identifying a focal point within DoD for Information Warfare activities to allocating 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 report concluded that the clearance process was needlessly complex, cumbersome, and costly. The Joint Security Commission report 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 (AISs)," March 21, 1988 (DoD Directive 5200.28), 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)*

Certification. Certification is the technical evaluation of an automated information system's security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular automated information system's design and implementation meet a set of specified security requirements. *(DoD Directive 5200.28)*

Contingency Planning. Contingency plans are required to be developed and tested in accordance with Circular A-130 to ensure that automated information system 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, procedures must be in place to recover. *(DoD Directive 5200.28)*

Interim Authority to Operate. The appropriate designated approving authority will accredit automated information systems, networks, and computer resources based on a certification and risk management process. Automated information systems not accredited may operate if the appropriate designated approving authority has issued an interim authority to operate for a period not to exceed 1 year. *(Secretary of the Navy Instruction 5239.2, "Department of the Navy Automated Information Systems (AIS) Security Program," November 15, 1989)*

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 Test and Evaluation. Systems shall be subjected to a site and system specific security test and evaluation to ensure that the environmental and operational security requirements have been met. When feasible, security test and evaluation should be conducted by a third party approved by the designated approving authority. (*Secretary of the Navy Instruction 5239.2*)

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

Vulnerability. Vulnerability is weakness in an information system or its components (system security procedures, hardware design, management controls) that could be exploited. (*National Security Telecommunications and Information Systems Security Instruction No. 4009*)

Key Officials

DoD Directive 5200.28 defines the responsibilities of key officials that affect automated information systems security.

Designated Approving Authority. The designated approving authority is the official who has the authority to decide whether to accept the security safeguards prescribed for an automated information system or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The designated approving authority must be at an organizational level, have authority to evaluate the overall mission requirements of the automated information system, and provide definitive directions to automated information system developers or owners relative to the risk in the security posture of the automated information system. (*DoD Directive 5200.28*)

Information Systems Security Manager. The information systems security manager is responsible for planning, directing, and implementing the information security program. The information systems security manager is administratively and operationally responsible for the computer system. Generally, each organization has one information systems security manager. (*Pearl Harbor Naval Shipyard Computer Security Handbook, 1996*)

Information System Security Officer. The information system security officer is responsible to the designated approving authority for ensuring that security is provided for and implemented. Specifically, the information system security officer is to:

- maintain a plan for system security improvements and progress towards meeting the accreditation,

Appendix C. Glossary

- evaluate known vulnerabilities to ascertain whether additional safeguards are needed, and
- ensure that audit trails are reviewed periodically. (*DoD Directive 5200.28*)

Terminal Area Security Officer. Terminal area security officers are appointed for computer systems with remote terminal access. The terminal area security officer provides security support to the information system security officer, and reports any problems or security compromises to the information system security officer. Terminal area security officers may also be assigned as an “assistant information system security officer” in areas where the number of systems exceeds the ability of one information system security officer to effectively administer security requirements. (*Pearl Harbor Naval Shipyard Computer Security Handbook, 1996*)

Appendix D. 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, 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)

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
Director, Human Resources Operations Center, Information Technology
Director, Human Resources Service Center, Pacific Region

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

Marine Corps

Director, Civilian Human Resources Office-West
Director, Human Resources Office Marine Corps Base Hawaii Kaneohe Bay

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

Department of the Navy Comments



THE ASSISTANT SECRETARY OF THE NAVY
(MANPOWER AND RESERVE AFFAIRS)
WASHINGTON, D.C. 20380-1000

APR 13 1998

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE,
DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Audit Report on Information Assurance of the Defense
Civilian Personnel Data System - Navy (Project No.
7RE-3006.02)

Attachment 1 was transmitted to the Director of Civilian
Personnel Programs, Headquarters, United States Marine Corps,
for review and comments.

The Department of the Navy concurs in the report finding
and recommendations. Detailed comments are contained in
Attachment 2.

A handwritten signature in cursive script, appearing to read "Bernard Rostker".
BERNARD ROSTKER

Attachments:

1. DoDIG Draft of A Proposed Audit Report: Information Assurance
of the Defense Civilian Personnel Data System - Navy (Project
No. 7RE-3006.02 of February 6, 1998)
2. Department of the Navy comments

Copy to:
FMO-31
NAVINGEN(02)

*Omitted because Attachment 1 is a copy of the draft report.

Department of the Navy Comments
on
DODIG Draft Audit Report
on
Information Assurance of the Defense Civilian
Personnel Data System
Project #7RE-3006.02

Finding: The Navy Pacific Region and two of its three human resources offices have made Defense Civilian Personnel Data System information assurance a high priority and have computer security programs in place. However, information assurance for its Human Resources Office, Marine Corps Base Hawaii, Kaneohe Bay still need improvement because it does not have an overall security plan and contingency plan.

DOH Reply: Concur.

Recommendation: "We recommend that the Director, Human Resources Office Marine Corps Base Hawaii Kaneohe Bay complete an overall security plan for the Defense Civilian Personnel Data System."

DOH Reply: Concur. A security plan is being developed at Kaneohe Bay which will ensure the integrity of the computer systems used to hold personnel data.

Recommendation: "We recommend that the Director, Human Resources Office Marine Corps Base Hawaii Kaneohe Bay complete a contingency plan for the Defense Civilian Personnel Data System."

DOH Reply: Concur. HRO Kaneohe Bay is working with the base Communication Information Systems Department to develop a contingency plan which will include backup security controls and data recovery systems.

Attachment 2

Civilian Personnel Management Service Comments



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

APR 06 1998

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT
DIRECTORATE, DEPARTMENT OF DEFENSE
INSPECTOR GENERAL

SUBJECT: Proposed Audit Report on Information Assurance for the Defense Civilian
Personnel Data System – Navy (Project No. 7RE-3006.02)

This memorandum constitutes the functional proponent's response to the Proposed Audit Report on Information Assurance for the Defense Civilian Personnel Data System – Navy, dated February 6, 1998 (Project No. 7RE-3006-02). 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 the Defense Civilian Personnel Data System program information. We appreciate your consideration of our comments.

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)-Navy
DoD IG Project No. 7RE-3006.02

AUDIT BACKGROUND

Defense Civilian Personnel Data System (page 2, first paragraph). "The Defense Civilian Personnel Data System (DCPDS) will provide a seamless automated information system for civilian personnel policy actions and personnel decisions during peacetime, contingencies, and wartime. The DCPDS will support Military Departments and Defense agencies worldwide and will be used by personnel officials, employees, managers, and senior leadership at all levels of DoD operations. The DCPDS resides on a mainframe computer and has up to three separate databases at Military Department or Defense agency levels to support civilian personnel operations. The DCPDS databases are maintained at the Air Force Information Processing Activity located at Randolph Air Force Base, San Antonio, Texas. The DCPDS will store, process, and transmit data for 750,000 personnel records, of which 209,000 belong to the Navy and Marine Corps and are subject to the Privacy Act of 1974 and the Freedom of Information Act. For security purposes, the DCPDS data re labeled "sensitive-but-unclassified."

Revised

Revised

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 recommend the substitution of the following language, which clarifies the distinction between the legacy DCPDS and the modern DCPDS. Also, the proposed language corrects a technical error, in that, the legacy DCPDS mainframes that support DoD Military Services and Federal Agencies (other than an Air Force portion) are not located at Randolph AFB, Texas.

"Defense Civilian Personnel Data System. The legacy Defense Civilian Personnel Data System (DCPDS) is an automated information system that is the standard DoD civilian personnel system. The legacy DCPDS is used to document and store civilian personnel actions for the Department's employees. The system processes sensitive-but-unclassified personnel information. The legacy DCPDS resides on a mainframe computer and has separate databases at Military Department or Defense agency levels to support civilian personnel operations. The legacy DCPDS databases are maintained at the Defense Information Systems Agency Defense Megacenter, San Antonio, located at Kelly AFB, Texas. DCPDS stores, processes and transmits data for 750,000 personnel records, of which 209,000 belong to the Navy and Marine Corps and are subject to the Privacy Act of 1974 and the Freedom of Information Act.

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 the legacy 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.

Civilian Personnel Management Service Comments

Final Report
Reference

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."

The Navy Regions (first paragraph). "The DCPDS will enable the Military Departments and the Defense agencies to process, store, and transmit civilian personnel records on databases at 23 regional service centers."

Response: There are 22 regional service centers under the current program. The Defense Mapping Agency regional service center, which achieved full operating capability in FY 1995, was realigned under the National Imagery and Mapping Agency (NIMA). Due to its change in security classification status NIMA is no longer counted as part of the regionalization program. Recommend the sentence be changed to read as follows:

"The modern DCPDS will enable the Military Departments and the Defense agencies to process, store, and transmit civilian personnel records on databases at 22 regional service centers."

The Navy Regions (paragraph 2). "Additionally, the Navy DCPDS database interfaces with other DoD and Federal functional databases; for example, payroll and the Office of Management and Budget."

Response: The Navy DCPDS does not have an interface with the Office of Management and Budget. The Navy DCPDS does provide data to the Headquarters Navy System, which, in turn, produces a tape to be sent to the Office of Personnel Management to update the Central Personnel Data File. Recommend that this sentence be revised to read:

"Additionally, the Navy DCPDS database feeds data to other DoD databases, for example Defense Civilian Payroll System and the Headquarters Navy System."

INFORMATION ASSURANCE PROGRAM:

Page 5, paragraph 2. "Further, the DCPDS functional and acquisition program managers did not coordinate with Navy about their respective security management roles and responsibilities for the DCPDS information assurance program."

Coordination with DoD Components (page 10, paragraph 6). "The DCPDS functional and acquisition project managers did not coordinate with the Navy in their respective security management roles and responsibilities for the DCPDS information assurance program."

Coordination with DoD Components (page 11, paragraph 4). "Coordination of DCPDS security issues is important to provide consistency among all DoD Components operating DCPDS. The lack of coordination is causing DoD Components to take their own approaches to security; that is, they are independently developing their own measures to deal with DCPDS vulnerabilities."

Revised

Revised

Response:

These three statements do not accurately reflect the work that has been accomplished by the functional and acquisition program managers with regards to security management roles and DCPDS information assurance. 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 and acquisition program managers did not modify the existing security management roles, responsibilities, and processes.

The Central Design Activity (CDA) located at the Air Force Personnel Center (AFPC), Randolph AFB, Texas has coordinated with the Components concerning the security management roles and responsibilities for the PPI Suite used in conjunction with the legacy DCPDS. The CDA also provided the Component systems administrators with training and manuals that cover practices and procedures for granting access to the PPI Suite. On February 12, 1997, the CDA provided Component systems administrators a software release announcement for PPI Version 4.4. This release implemented the first scripts to configure servers and workstations in accordance with the established security policy. The CDA 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.

As previously stated, the Department is now in the process of developing the modern DCPDS. The functionality of the PPI Suite will be included in the modern system. Recently, a coordinated modern DCPDS policy and security support plan was published. This document clearly defines the respective security management roles and responsibilities for the modern DCPDS.

CPMS, in conjunction with the CDA security staff, is developing a System Security Annex to the Training Support Plan (TSP). The Annex will be provided to Components, in order to plan, develop, and execute training strategies for functional and technical personnel involved in the operations of the modern DCPDS. The Annex also contains the knowledge, skills and abilities and training requirements for network security personnel, system administrators, database administrators, information system security officers, and users at all operational levels. The Annex will be completed by April 30, 1998.

Added

Added

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

