October 11, 2002

Information System Security

Security Controls for the Defense Procurement Payment System

(D-2003-009)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General of the Department of Defense Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

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

Acronyms

AIS	Automated Information System
COOP	Continuity of Operations Plan
DAA	Designated Approving Authority
DCD	Defense Finance and Accounting Service Corporate Database
DCII	Defense Finance and Accounting Service Corporate Information Infrastructure
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology System Certification and Accreditation Process
DPPS	Defense Procurement Payment System
GISRA	Government Information Security Reform Act
MOA	Memorandum of Agreement
PMO	Program Management Office
SLA	Service Level Agreement
SSAA	System Security Authorization Agreement

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

October 11, 2002

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Report on Security Controls for the Defense Procurement Payment System (Report No. D-2003-009)

We are providing this report for your review and comment. We considered management comments on the draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all issues be resolved promptly. Management comments were partially responsive. As a result of management comments, we revised Recommendation 6. to clarify our intent that management should specifically implement the provisions of the DoD Information Technology Security Certification and Accreditation Process to bring the Defense Procurement Payment System in full compliance with the requirements of the Government Information Security Reform Act. We request that management provide comments on Recommendation 6. by November 29, 2002.

If possible, please provide management comments in electronic format (Adobe Acrobat file only). Send electronic transmission to the e-mail addresses cited in the last paragraph of this memorandum. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the classified SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. David F. Vincent at (703) 604-9109 (DSN 664-9109) (dvincent@dodig.osd.mil) or Ms. Barbara A. Sauls at (703) 604-9129 (DSN 664-9129) (bsauls@dodig.osd.mil). See Appendix B for the report distribution. The team members are listed inside the back cover.

for David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2003-009 **October 11, 2002**
(Project No. D2002FH-0007)

Security Controls for the Defense Procurement Payment System

Executive Summary

Who Should Read This Report and Why? Information technology professionals who are responsible for system development and system changes and prospective users of systems under development or undergoing major modifications will be most interested in the progress of the program discussed in this report.

Background. On May 21, 1997, the Under Secretary of Defense (Comptroller)/Chief Financial Officer directed the move to a paper-free contracting process, which would modernize the acquisition processes of contract writing, administration, finance, and auditing. The Defense Finance and Accounting Service initiated the Defense Procurement Payment System (DPPS) as part of the DoD Paper-Free Contracting Initiative. This report addresses the system's compliance with DoD security policy. DPPS is a component of the information infrastructure architecture and is an Oracle-based Federal financial system that uses standard, shareable data. DPPS will eliminate the need for multiple systems that process contract and vendor payments. As of April 2002, the total dollar value expended for system development was $80 million. The life-cycle costs are estimated to be $550.5 million.

Results. The Defense Finance and Accounting Service did not provide reasonable assurance that the general security controls for the initial development of DPPS were adequate. DPPS did not fully implement the requirements to be reviewed under the Government Information Security Reform Act and if fielded as is would operate without basic security elements such as proper access controls and a contingency plan. As a result, existing weaknesses may lead to unauthorized access by potential users that may result in undetected alteration or misuse. Those weaknesses may also cause DPPS to negatively impact the Defense Finance and Accounting Service Corporate Information Infrastructure system interoperability. To improve system security and eradicate existing weaknesses, the DPPS Program Management Office should:

- revise the System Security Authorization Agreement and the memorandum of agreement in accordance with the current directive,
- review security documents of the Defense Corporate Database,

- test the continuity of operations plan for the system,
- develop standard operating procedures for obtaining access to the system, and
- implement fully the provisions of the DoD guidance to bring the system into full compliance with the Government Information Security Reform Act.

See the Finding section of the report for details on the audit results and complete detailed recommendations.

Management Comments and Audit Response. The Defense Finance and Accounting Service Chief Information Officer concurred with the finding and recommendations and agreed to implement the requirements necessary to improve the system security of the Defense Procurement Payment System. Management comments were partially responsive. We cannot be certain that all requirements of the Government Information Security Reform Act will be met. Accordingly, we revised the recommendation to clarify our intent that the Defense Finance and Accounting Service Chief Information Officer should implement the provisions of the DoD Information Technology Security Certification and Accreditation Process. This would ensure that the Defense Procurement Payment System is in full compliance with the Government Information Security Reform Act. We request that the Defense Finance and Accounting Service Chief Information Officer provide comments on the final report by November 29, 2002.

Table of Contents

Executive Summary i

Background 1

Objectives 3

Finding

Security Controls for the Initial Development of the Defense Procurement Payment System 4

Appendixes

A. Scope and Methodology
Management Control Program Review 15
Prior Coverage 16
B. Report Distribution 17

Management Comments

Defense Finance and Accounting Service 19

Background

Origin of the Defense Procurement Payment System. On May 21, 1997, the Under Secretary of Defense (Comptroller)/Chief Financial Officer directed the move to a paper-free contracting process, which would modernize the acquisition processes of contract writing, administration, finance, and auditing. The Defense Finance and Accounting Service (DFAS) initiated the Defense Procurement Payment System (DPPS) as part of the DoD Paper-Free Contracting Initiative. The mission need for DPPS was derived from the DFAS Strategic Business Plan and Chief Financial Officer 5 Year Plan to improve systems' capabilities and business processes for finance and accounting. The vision for DPPS is to modernize business processes and define standard and shareable data for contract and vendor payments. DPPS should alleviate the need for multiple systems currently used for contract and vendor payments. Through DPPS, contract and vendor payments will be integrated into a standardized on-line computer-processing environment. DPPS will merge both functional areas to operate from common data rather than duplicated or unmatched data records residing in various databases and in hard copy form.

In April 1995, DFAS initiated the DPPS program. In September 1996, DFAS decided to purchase a commercial off-the-shelf package for DPPS instead of developing the DPPS software. In June 1998, DFAS decided to purchase an Oracle-based project. The commercial off-the-shelf award was $24 million, and the commercial off-the-shelf package was $5.7 million. As of April 2002, the total dollar value expended including salaries was $80 million. DFAS expended $51 million of the total dollar value on Oracle obligations. The estimated life-cycle costs are $550.5 million. Currently, DPPS is under Milestone 2 approval and is expected to reach Milestone 3 approval by September 2003.

Interfacing Systems and Procurement Process. Figure 1 shows how data will be processed through DPPS. DPPS will directly or indirectly interface with the following systems through the DFAS Corporate Information Infrastructure (DCII): DFAS Corporate Database (DCD), Defense Standard Disbursing System, Standard Procurement System, and Wide Area Workflow.

DPPS is one of many systems that encompass the DCII environment. DCII is an enterprise architecture that modernizes and integrates the financial operations using DoD-wide standard software initiatives that operate on a standard infrastructure. DCD will serve as the main hub to process data received from all systems. The function of DCD is to consolidate data from several systems into one standard manner. DPPS is an Oracle-based Federal financial system that uses standard, shareable data and the most recent advances in e-commerce.

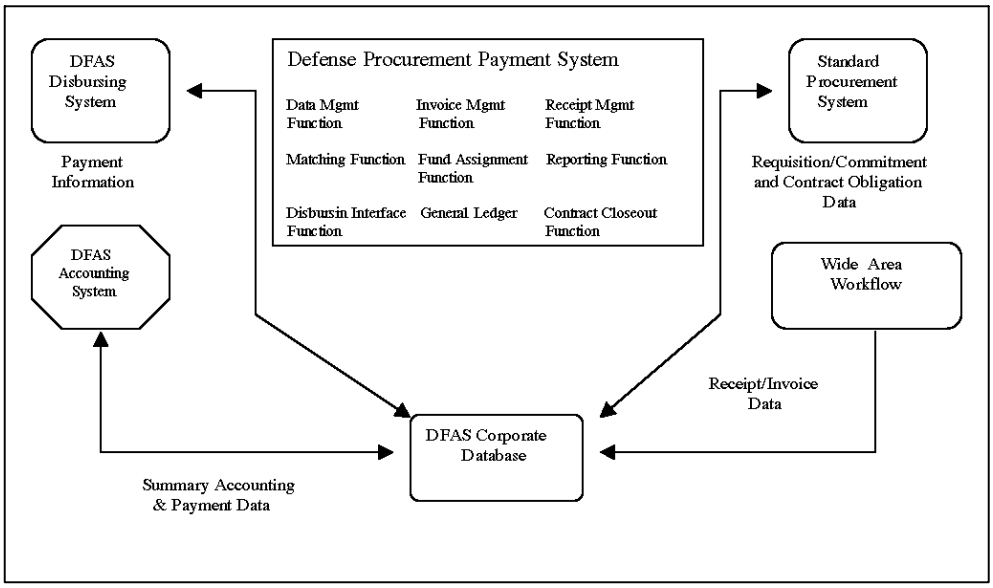

Figure 1. DPPS Processing Flow

DPPS has been modified to function in the DFAS environment and will become the standard entitlement system. DPPS will eventually replace the entitlement function for a number of systems to include the:

- Automated Voucher Examination and Disbursing System,
- Computerized Accounts Payable System,
- Defense Integrated Subsistence Management System,
- Integrated Accounts Payable System,
- Mechanization of Contract Administration Services,
- Standard Automated Material Management System,
- Standard Automated Voucher Examination System, and
- Standard Accounting and Reporting System.

Once functional, DPPS will receive contract, receipt, invoice, and funding data authorization from DCD. DPPS will also send data to DCD.

Objectives

The overall objective was to evaluate the adequacy of the DPPS security controls. The audit included a review of general controls. We also reviewed the adequacy of the management control program as it related to the overall audit objective. See Appendix A for details on the scope and methodology, management control program, and prior audit coverage.

Security Controls for the Initial Development of the Defense Procurement Payment System

DFAS did not provide reasonable assurance that the general security controls for the initial development of DPPS were adequate. This occurred because in its initial development of DPPS, DFAS did not properly implement the first two phases of the DoD security guidance for system security and accreditation. Specifically, DFAS did not address the minimum-security requirements in the System Security Authorization Agreement (SSAA) to include the weaknesses identified in the DCD system. In addition, critical documents required in the SSAA; such as the continuity of operations plan (COOP), the memorandum of agreement (MOA), the service level agreement (SLA), and the roles and responsibilities of users; did not contain the information needed to ensure the security of DPPS. DPPS did not fully implement the requirements to be reviewed under the Government Information Security Reform Act (the Act) and, if fielded as is, would operate without basic security elements such as proper access controls and a contingency plan. As a result, data integrity may be compromised because of system availability, unauthorized access, undetected alteration, or general misuse. Although DFAS may correct all shortfalls prior to the deployment of DPPS, the time needed to make the system changes necessary to properly secure DPPS may negatively impact interoperability of the DCII system.

Security Guidance

General Provisions of the Government Information Security Reform Act. The October 30, 2000, Floyd D. Spence National Defense Authorization Act of FY 2001 (Public Law 106-398), includes title X, subtitle G, "Government Information Security Reform Act," (GISRA). The GISRA states that each Federal agency is responsible for:

- implementing a security program that ensures the integrity, confidentiality, authenticity, availability, and nonrepudiation of information systems supporting agency operations;
- ensuring that the information security plan is followed throughout the life cycle of the system; and
- developing, implementing, and evaluating information security policies and control techniques.

Office of Management and Budget Guidance. Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources," November 30, 2000, establishes a minimum set of controls to be included in the Federal automated information security program. The Office of Management and Budget guidance also assigns responsibility for

security, security planning, periodic review of security controls and links, agency automated information security programs, and agency management control systems. In addition, the guidance should ensure that risk and potential for loss are understood and minimized.

DoD Directive 5200.28. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988, states that the security policy must be considered throughout the entire life of the AIS from the beginning of concept development, through design, development, operation, and maintenance until replacement or disposal. A Designated Approving Authority (DAA) shall be designated as responsible for the overall security of the AIS to include approval of accreditation. The AIS developer must ensure early and continuous involvement of the users, information system security officers, data owners, and DAA(s) in defining and implementing security requirements of the AIS. The AIS developer should also develop an evaluation plan for the AIS showing progress toward meeting full compliance with stated security requirements through the use of necessary computer security safeguards. DoD Directive 5200.28 also states that an MOA should be implemented when one DoD Component AIS interfaces with another DoD Component AIS. The MOA should include a description and classification of the data, clearance levels of the users, designation of the DAA who should resolve conflicts among each DAA, and safeguards to be implemented before interfacing each AIS. DoD Directive 5200.28 is necessary to protect the DoD investment in obtaining and using information and to prevent fraud, waste, and abuse.

DoD Information Technology System Certification and Accreditation Process Instruction. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, defines four phases that lead to the system security and accreditation process. Phase 1 requires the establishment of an SSAA among each DAA, Certification Authority, system user representatives, and the program manager. The SSAA documents agreements among the parties relating to system mission, environment, architecture, threats, levels of effort, and security requirements for certification and accreditation. Phase 2 activities verify the evolving systems compliance with the requirements agreed on in the SSAA. Phase 3 activities validate that the preceding work has produced an information system that operates in a specified computing environment with an acceptable level of residual risk. Phase 4, the Post Accreditation phase, contains activities necessary to monitor system management and operation to ensure an acceptable level of residual risk is preserved.

DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual." DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process Application Manual," July 31, 2000, is issued under the authority of DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997. It provides implementation guidance to standardize the certification and accreditation process throughout DoD.

DFAS System Security Guidance. DFAS Regulation 8000.1-R, "DFAS Information Assurance Policy," as revised, November 1, 2001 (the Regulation), implements the information assurance policies stated in Circular No. A-130. The Regulation provides the structure for carrying out security policies, responsibilities, and procedures for DFAS systems security personnel, which all DFAS sites and programs are required to follow. The Regulation also establishes the DFAS Chief Information Officer as the DAA for all DFAS networks and information systems.

After reviewing guidance regarding security controls over automated information systems, we found problems with the adequacy of the SSAA developed for DPPS. Specifically, DFAS did not address the minimum-security requirements outlined in DoD guidance. The minimum-security requirements that were not addressed in the SSAA involve risk management, contingency planning, data integrity, accountability and access controls, and least privilege. Security requirements should be followed so that only authorized persons can access information and the information is used for its intended purpose. Security requirements should also ensure that information retains its content integrity and is available when needed.

Security Controls Over DPPS

Adequacy of DPPS System Security Authorization Agreement. DoD Directive 5200.28 states that the DAA is responsible for the overall security of DPPS. The DAA for DPPS is the Chief Information Officer for DFAS. DFAS develops the DPPS and is responsible for ensuring that the security requirements for its input, access, and use are adequate. However, the DAA did not provide reasonable assurance that the security controls for the initial development of DPPS were adequate. The DPPS SSAA is a documented agreement of the certification process that is developed by the Program Management Office (PMO). The SSAA required for review by the DAA for certification and accreditation did not adequately address the minimum-security safeguards outlined in DoD Directive 5200.28. Specifically, the SSAA is non-compliant with several major requirements of the DITSCAP. The SSAA did not give a detailed description of the threats that DPPS faces. The DPPS COOP, a part of the SSAA, did not adequately implement service continuity controls to ensure that critical and sensitive data will be protected, and that essential operations would continue in an emergency. The MOA between DPPS and DCD was not complete. The SLA between DFAS and the Defense Information Security Agency (DISA) was also not complete. As of March 2002, the roles and responsibilities for DPPS had not been assigned or tested. The following table provides a list of the specific security requirements for DPPS. The SSAA was generic and did not adequately document the specific requirements of DPPS.

Mandatory DPPS Certification and Accreditation Requirements

Specific Security Requirements for DPPS	Adequate
Specific contingency plan for DPPS	No
Specific risk assessment for DPPS	No
Specific network and physical security	Yes
Specific accreditation survey for DPPS	No
Specific configuration management program	No
Specific security program for DPPS	Yes
Specific memorandum of agreement	No
Specific Service Level Agreement	No
Specific Certification Analysis	Yes
Specific Roles and Responsibilities for DPPS	No

DPPS Vulnerabilities. As part of the DCII, DPPS will receive data from multiple sources via the DCD interface. The DCD is the central component in the DoD end-to-end procurement process. Once the disbursing functionality is deployed, the DCD will provide a single, logical database in which all shared DFAS financial data will be stored and maintained for on-line transaction processing. The DCD, as well as the DPPS, is part of the target-automated environment along with other systems. Those systems will share data using the DCD. DFAS officials stated that if the DCD experienced a failure, DPPS would not have the necessary data to operate.

Inspector General DoD Report No. D-2002-067, "Security Controls Over the Defense Finance and Accounting Service Corporate Database," March 20, 2002, addresses security issues found during a review of security controls of the DCD. In the report, several weaknesses were found in the execution of DCD security controls. Specifically, the report stated that access controls were weak, a training program for users was not provided, and the COOP had been in draft since 1999. In addition, the COOP had not been tested at the time the report was issued. Prior to fielding the DCD, neither a system security review nor penetration testing were requested. Figure 2 illustrates the procurement process in the DCII environment.

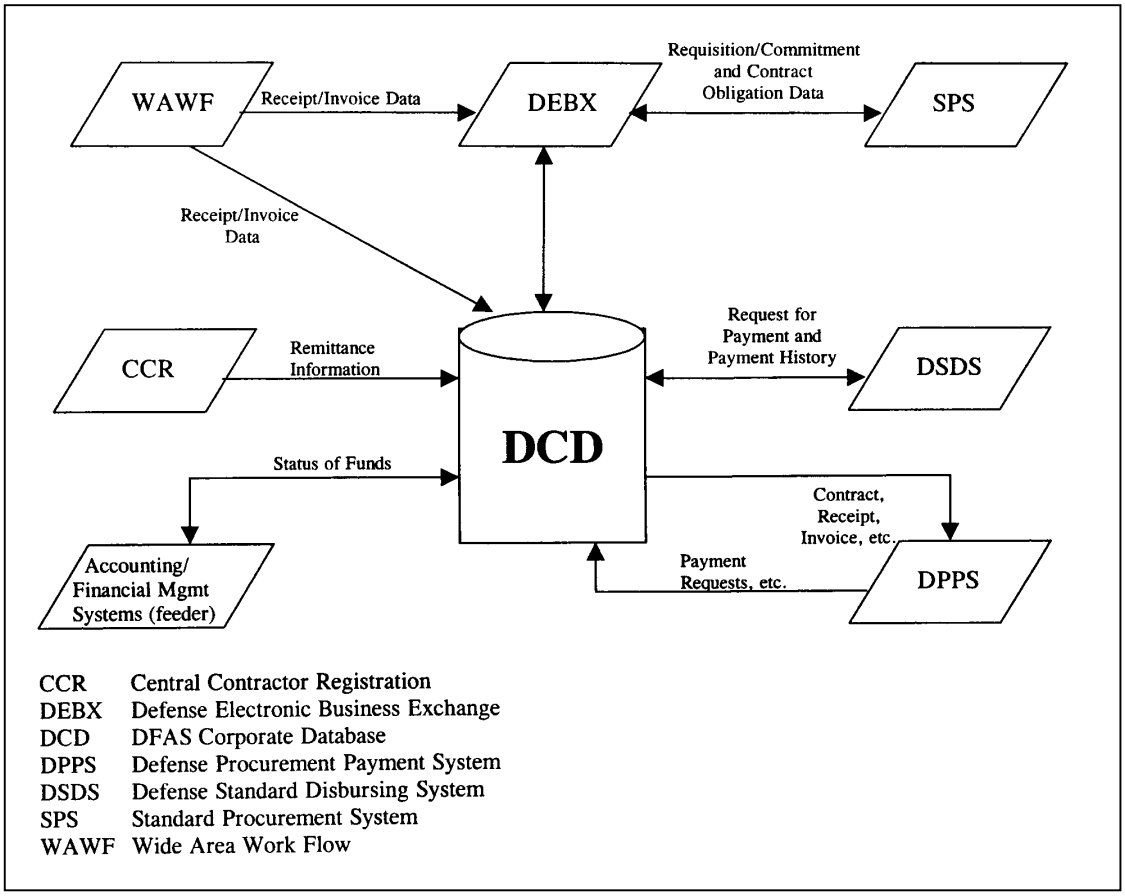

Figure 2. DFAS Corporate Database Interfaces

The DPPS PMO was not aware of the inadequate security safeguards in the DCD. The PMO requested and received a copy of the Inspector General DoD Report No. D-2002-067 that discussed the security controls weaknesses in the DCD. The PMO found that the problems in the DCD would be relevant to DPPS. As of April 2002, the weaknesses identified in the DCD had not been included in the DPPS SSAA. The threats discussed in the DPPS SSAA were general to the DCII environment. The SSAA did not include the security plans for the other applications in the DCII environment.

During Phase 2 of the DITSCAP process, certification tasks and a vulnerability assessment are to be performed. For DPPS, the vulnerability assessment task noted the following weaknesses.

- The current version of the application may not provide for recommended encryption levels.

- The application does not enforce "strong" passwords, which could lead to hacking incidents and loss of data integrity.

- The audit fields may not properly capture the data necessary to verify transactions.

- The data may not be extractable for audit.

To achieve accountability and prevent fraudulent transactions from occurring, the weaknesses must be corrected. The PMO may recommend that the certification process continue while monitoring the mitigation of the vulnerabilities. The length of time needed to correct the vulnerabilities may slow the process, which leaves the security of DPPS in question. Additionally, some of the vulnerabilities were rated serious enough to recommend that the system not be deployed until they are corrected.

DPPS Continuity of Operations Plan. A COOP is required as part of the documentation developed during the certification and accreditation process. The objective of the COOP is to provide reasonable continuity of automated information systems support if events occur that prevent normal operations. Each COOP should be tested periodically under realistic conditions. The requirements of DoD Instruction 5200.40 state that the COOP should be prepared during Phase 1 of the certification and accreditation process. DoD Instruction 5200.40 further states that the COOP should be evaluated for feasibility during Phase 2 and again during Phase 3 to ensure consistency with the requirements set forth by the SSAA. According to the SSAA, Phase 2 of the certification and accreditation process had occurred during December 2001. During Phase 2, DFAS officials did not have a COOP for DPPS in place. Documentation of a COOP was not received until January 2002, but was dated June 2002, which, according to DFAS officials, will be the end of Phase 3. Although the COOP states that it will be tested and that test plans will be developed, no dates are included stating when the testing will occur. Furthermore, the plan does not contain the information necessary for testing, such as a Business Line COOP and a completed point of contact list in case of an emergency.

The Business Line COOP should encompass essential day-to-day operations of the user representative. Specifically, the Business Line COOP should identify step-by-step business functions necessary to ensure that contractor and vendor payments will be made despite the non-availability of DPPS. The lack of a Business Line COOP places a scope limitation on the DPPS COOP developed by the PMO. Without a Business Line COOP, DFAS cannot ensure that contractor and vendor payments will continue if DPPS becomes unavailable.

The DPPS COOP lacked a completed point of contact list. Specifically, officials with the authority to declare an emergency and implement the DPPS COOP were not identified. Further, the names of the officials to be contacted during the declaration of an emergency were not identified. The DPPS COOP contains just enough information to be considered adequate for Phase 1 of the certification and accreditation process but not for Phase 3 of DPPS. The lack of essential information limits the ability of the COOP to be tested for adequacy and its compliance with security requirements established in the SSAA.

DPPS/DCD Memorandum of Agreement. DoD Directive 5200.28 states that when an AIS is managed by a different DAA, or are interfaced or networked, an MOA is required to address the accreditation requirements for each AIS involved. The MOA should include description and classification of the data, clearance levels of the users, designation of the DAA who shall resolve conflicts among the DAAs, and safeguards to be implemented before interfacing each AIS. The MOA is established to ensure that an accurate and timely transfer occurs between two systems. An MOA is required any time that two DoD Component AISs interface with one another. An MOA is also required when a contractor AIS interfaces with either a DoD Component or to another contractor AIS.

The DPPS/DCD MOA does not adequately meet the requirements of DoD Directive 5200.28. The MOA states that Oracle Advanced Symmetrical Replication will facilitate the movement of data between DPPS and DCD. The MOA adequately describes how data will transfer between the systems and interfaces; however, it does not discuss the clearance levels of the users. Each clearance level for every system and its user should be clearly documented as a safeguard to prevent unauthorized access to both the DPPS and the DCD. In addition, the MOA does not clearly assign a DAA. The responsibility of the DAA includes resolving conflicts with each DAA of the respective systems.

DPPS Roles and Responsibilities. According to the DITSCAP, all certification team's roles and responsibilities are to be identified for the certification process and defined prior to end-to-end testing. A Role Assignment Matrix is being developed to include both the functional and administrative roles for the DPPS release. The matrix will also include job descriptions for DPPS, as well as clearance levels required for those positions. End-to-end testing for DPPS was scheduled to begin in March 2002. However, DFAS had not finalized the roles and responsibilities for DPPS.

Unless the roles and responsibilities are finalized, the Security Test and Evaluation cannot adequately test the roles and responsibilities for DPPS. The Security Test and Evaluation involves the testing of the setting up and managing of user profiles. Furthermore, without the establishment of the roles and responsibilities, access control issues cannot be achieved. Specifically, the roles and responsibilities are the development of a master access control list and coordination with DISA on user identification.

DPPS Service Level Agreement. DFAS is using the SLA as a guideline to meet DPPS security requirements. The SLA documents the agreement reached between DISA and DFAS. The agreement will provide information technology data processing support and customer support in the performance of a variety of information technology services, and DFAS. The SLA has three separate but interrelated parts, a basic agreement, a support agreement, and a planning estimate.

Basic Agreement. The basic agreement identifies terms, conditions, and responsibilities and incorporates standard information that applies to all DISA customers. It outlines administrative responsibilities, customer assistance, continuity of operations, and overall security. The basic agreement should have all the essential elements of a complete agreement and describe the

overall responsibilities of both parties. The basic agreement will also serve as the basic reference document for the support agreement between provider and customer.

Support Agreement. The support agreement documents the customer's requirements and the provider's technical solutions. The support agreement may also document any additions or modifications to the terms and conditions or roles and responsibilities covered in the basic agreement. Once signed, the agreement will remain in effect until jointly modified by the customer and provider or until terminated by either party.

Planning Estimate. The planning estimate classifies all projected workload costs for services provided by DISA. The cost estimates will be based on the most current workload projections provided by the customer.

The SLA between the DPPS PMO and DISA did not contain all of the necessary security information. The basic agreement outlines the responsibilities for DFAS and DISA pertaining to access controls. The SLA states that DFAS is responsible for maintaining access control for users of their applications. In addition, the SLA states that DISA will maintain access control based on required personnel security investigations, need-to-know, and authorization. However, the SLA does not outline the necessary procedures that either organization will follow to maintain access control. The SLA should explain the process for granting, generating, and maintaining access to DPPS. Otherwise, the intended users of DPPS could implement inconsistent access control procedures.

Compliance with the General Provisions of Government Information Security Reform Act. The Government Information Security Reform Act (the Act) directs each Federal agency to evaluate its information security program and practices annually and, as part of the budget process, submit the results to the Office of Management and Budget. The Act covers unclassified and national security systems to create a consistent security management framework for each system. The Act establishes parallel requirements for the agency and the agency Inspector General. The Act requires the Office of the Inspector General to evaluate the DoD information security program and practices and to independently select and test a subset of systems to confirm the effectiveness of the information security program. Although DPPS is not part of the subset of systems, DPPS compliance with the Act is still required.

DPPS is currently under Milestone 2 approval and is expected to reach Milestone 3 approval by September 2003. As a result, DPPS did not fully implement the requirements to be reviewed under the Act. For example, the PMO should report any material weaknesses in policies and procedures and system design and implementation.

Specifically, in order to comply with the Act, the PMO should:

- assess any risk to operations and assets,
- determine the level of security appropriate to protect the operations and assets, and
- develop and maintain an up-to-date security plan for DPPS.

If fielded as is, DPPS would operate without basic security elements to include proper access controls and a contingency plan. Before DPPS is fielded, the PMO should also ensure that employees are sufficiently trained in their security responsibilities and that procedures are established for reporting security incidents. If the PMO takes full advantage of this opportunity to ensure compliance with the Act, both the users of DPPS as well as the PMO will have a solid basis for stating that DPPS is ready for certification and accreditation.

Impact of DPPS on the DCII Environment

Delays in the development of DPPS have impacted the deployment of the DCII architecture. According to documentation provided by DFAS officials, DPPS was originally expected to take over the duties of the Mechanization of Contract Administration Services in February of 2000. However, delays in the development of the system have pushed back the "brownout of the Mechanization of Contract Administration Services" until the second quarter of FY 2003. More recent delays have been caused as well. Enterprise testing; which involves validating architecture for release build, data migration, and system security; was delayed because application testing of DPPS was not completed. Those tests uncovered defects and additional requirements for DPPS. If DPPS is not properly secured, DFAS may not be able to provide a secure end-to-end procurement process. Without adequate safeguards, the confidentiality and integrity of the information processed, stored, and transmitted, as well as the availability of the system or the information itself could be threatened, thus, risking the security of both the data in DPPS and the data transferable to the DCD.

Conclusion

DPPS is critical to the DFAS mission because when it is fully deployed, it will become the standard entitlement system, replacing several systems currently in use. As part of the DCII architecture, DPPS will receive and transfer data through the DCD from multiple sources. Because data are transferred to and from DPPS, any failure of DPPS would affect those interfacing systems. Therefore, it is important that DPPS has adequate security controls in place. DPPS will have thousands of users throughout the world. DFAS personnel will rely on DPPS to carry out their mission by providing access to financial applications and databases

and other information resources found in the DCD. In addition, without a properly tested COOP in place, there is no assurance that DPPS would continue to function in an emergency.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. As a result of management comments, we revised Recommendation 6 to clarify the actions necessary to bring the Defense Procurement Payment System into full compliance with the requirements of the Government Information Security Reform Act.

We recommend that the Defense Finance and Accounting Service Chief Information Officer direct the Defense Procurement Payment System Program Management Office to:

1. Revise the System Security Authorization Agreement for Defense Procurement Payment System to comply with DoD Directive 5200.28.

Management Comments. The Defense Finance and Accounting Service Chief Information Officer concurred and agreed to update the System Security Authorization Agreement and address security requirements from the DoD Directive 5200.28.

2. Review the security documentation such as test results and audit reports related to the Defense Finance and Accounting Service Corporate Database security.

Management Comments. The Defense Finance and Accounting Service Chief Information Officer concurred and will review the Defense Finance and Accounting Service Corporate Database security documentation.

3. Revise, finalize, and test the Defense Procurement Payment System Continuity of Operations Plan.

Management Comments. The Defense Finance and Accounting Service Chief Information Officer concurred and stated that the Continuity of Operations Plan for the Defense Procurement Payment System will be incorporated with the Defense Finance and Accounting Service Corporate Information Infrastructure plan and will be part of a tabletop exercise scheduled for September 2002.

4. Revise the Defense Procurement Payment System memorandum of agreement to comply with DoD Directive 5200.28.

Management Comments. The Defense Finance and Accounting Service Chief Information Officer concurred and agreed to update the memorandum of agreement to clarify the Designated Approving Authority responsibilities and any security clearance levels in their roles using both systems.

5. Develop a standard operating procedure for obtaining access to the Defense Procurement Payment System.

Management Comments. The Defense Finance and Accounting Service Chief Information Officer concurred and stated that the Defense Finance and Accounting Service Corporate Information Infrastructure access control standard operating procedures have been written to combine the Defense Corporate Database, the Defense Corporate Warehouse, and the Defense Procurement Payment System. The procedures are currently awaiting final approval. These standard operating procedures define the least privilege concept and roles and responsibilities.

6. Implement fully the provisions of the DoD Information Technology Security Certification and Accreditation Process to bring the Defense Procurement Payment System into full compliance with the requirements of the Government Information Security Reform Act.

Management Comments. The Defense Finance and Accounting Service Chief Information Officer concurred with the recommendation and stated that the Defense Procurement Payment System complied with the Government Information Security Reform Act by providing the Defense Finance and Accounting Service management with all requested information needed to fulfill the requirements. The Fiscal Year 2003 Budget Estimate also contains the required information.

Audit Response. Management comments were partially responsive. Although the Defense Finance and Accounting Service Chief Information Officer provided the Defense Finance and Accounting Service management all information requested, we can not be certain that all requirements of the Government Information Security Reform Act will be met. As a result, we revised the recommendation to clarify our intent that the Defense Finance and Accounting Service Chief Information Officer should implement the provisions of the DoD Information Technology Security Certification and Accreditation Process to bring the system in full compliance with the requirements of the Government Information Security Reform Act. We request that the Defense Finance and Accounting Service Chief Information Officer provide comments on the final report.

Appendix A. Scope and Methodology

We performed this financial-related audit at the DPPS PMO at DFAS Columbus, Ohio, from October 2001 through May 2002. Our review was based on applicable Federal and DoD information security guidance and regulations. We used the DITSCAP criteria for evaluating the SSAA for DPPS. We reviewed the process in which DFAS intends to implement its security program, access controls, and service continuity for DPPS. We interviewed the DAA for DPPS, project director for the DCII, project manager for DPPS, and the user representatives. We interviewed the DPPS Information System Security Officer to determine how they plan to implement security over DPPS.

We reviewed the DPPS SSAA of August 2001 and supporting documentation. We also analyzed the SLA between DFAS and DISA. We reviewed the MOA between DPPS and DCD, dated December 30, 2001. The DPPS COOP that we reviewed was post dated June 2002. We reviewed relevant regulations and laws including Public Law 100-235, "Computer Security Act of 1987," and the requirements of the Government Information Security Reform Act, title X, subtitle G, of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). Additionally, we reviewed DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988; DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997; DoD 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000; and DFAS Regulation 8000.1-R, "DFAS Information Assurance Policy," as revised, November 1, 2001.

We performed this audit from October 2001 through July 2002, in accordance with generally accepted government auditing standards. Accordingly, we included tests of management controls considered necessary.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Security and the DoD Financial Management high-risk areas.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We reviewed the adequacy of management controls for the initial development of DPPS. Specifically, we reviewed the FY 2001 DFAS Annual Statement of Assurance and the FY 2001 Contract Pay and Vendor Pay Services Annual Statement of Assurance for DFAS Columbus.

Adequacy of Management Controls. We identified material management control weaknesses for DFAS as identified in DoD Instruction 5010.40. DFAS did not provide reasonable assurance that the general security controls for the initial development of DPPS were adequate. The recommendations in this report, if implemented, will improve the security controls over DPPS. A copy of the report will be provided to the senior official responsible for management controls at DFAS Headquarters.

Adequacy of Management's Self-Evaluation. We reviewed the adequacy of management's self-evaluation. DFAS officials did not identify DPPS as an assessable unit; therefore, did not identify or report the material management control weakness identified by the audit.

Prior Coverage

General Accounting Office

GAO-01-525, "Information Technology: Architecture Needed to Guide Modernization of DoD's Financial Operations," May 17, 2001.

GAO-01-307, "Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program," March 30, 2001.

Inspector General of the Department of Defense (IG DoD)

IG DoD, Report No. D-2002-067, "Security Controls Over the Defense Finance and Accounting Service Corporate Database," March 20, 2002.

IG DoD, Report No. D-2001-095, "Controls for the Electronic Data Interchange at the Defense Finance and Accounting Service Columbus," April 6, 2001.

IG DoD, Report No. D-2001-030, "Oversight of the Defense Finance and Accounting Service Corporate Database Development," December 28, 2000.

IG DoD, Report No. 98-007, "General and Application Controls Over the Mechanization of Contract Administration Services System," October 9, 1997.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Department of the Army

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

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

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

Other Defense Organizations

Director, Defense Finance and Accounting Service
    Defense Finance and Accounting Service Columbus

Non-Defense Federal Organizations and Individuals

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

SEP 17 2002

DFAS-DSDP/CO

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to Department of Defense (DoD) Inspector General Report on "Security Controls for the Defense Procurement Payment System" (Project No. D2002FH-0007)

The Defense Procurement Payment System (DPPS) Program Management Office provides this response to the above named audit. In general, the program office concurs with the recommendation in the report. Our comments are provided below.

It should be noted that the recommendations in this report were always known to DPPS and a plan has been in place to comply. At the time the audit was conducted, the program was not at the stage in which the recommendations would have been enacted to the level of detail sufficient to render a more conclusive assessment.

1. Revise the System Security Authorization Agreement for Defense Procurement Payment System to comply with DoD Directive 5200.28

   Management Comments: Concur. The SSAA is under continuous review and revision. The SSAA that was under IG review was dated August 2001. It contained the most current information that was available at that time for a developing system. When development ends and prior to receiving authority to operate, the SSAA will be updated and will address the security requirements from DoD Directive 5200.28.

   Estimated Completion Date: November 2002

2. Review the security documentation such as test results and audit reports related to the Defense Finance and Accounting Service Corporate Database Security.

   Management Comments: Concur. DPPS is in contact with the DCD ISSO and DCII Security Manager and is taking advantage of "Lessons Learned" from other DCII system's audits as well as sharing test results from the Enterprise Test. DPPS will review DCD/DCII security documentation as it pertains to DPPS.

   Estimated Completion Date: November 2002

3. Revise, finalize, and test the Defense Procurement Payment System Continuity of Operations Plan.

   Management Comments: Concur. Because of the integrated nature of the DCII, DPPS will be incorporated into a DCII COOP. Specific DPPS Information will be included in Appendix O of the DCII COOP. The final DCII COOP will be tested in OT&E, prior to requesting a Milestone III decision. A series of preliminary tabletop exercises are planned to refine the COOP. The schedule for the tabletop COOP exercises is being coordinated with JITC. The next DCII COOP tabletop exercise is scheduled for September 2002.

   Estimated Completion Date: September 2002

Your Financial Partner @ Work
www.dfas.mil

Final Report Reference

4. Revise the Defense Procurement Payment System Memorandum of Agreement to comply with DoD Directive 5200.28

   Management Comments: Concur. The current DPPS/DCD Memorandum of Agreement will be updated to clarify the DAA responsibilities and any security clearance levels in their roles using both systems.

   Estimated Completion Date: November 2002

5. Develop a standard operating procedure for obtaining access to the Defense Procurement Payment System.

   Management Comments: Concur. A combined DCII Access Control Standard Operating Procedures (SOP) has been written (covering DCD, DCW, and DPPS) and is currently at DFAS Arlington for signature. These procedures define use of the access request DISA SAAR form, supervisory and data owner approval based on the least privilege concept, as well as roles and responsibilities. This SOP has been drafted by and is presently being evaluated and tested by DCII Production Support Office and DFAS Infrastructure Services Organization in conjunction with the DCII Enterprise Test.

   Estimated Completion Date: September 2002

Revised Page 14

6. Review the requirements of the Government Information Security Reform Act and ensure the Defense Procurement Payment System complies with the Act.

   Management Comments: Concur. A purpose of the Government Information Security Reform Act is to provide a mechanism for improved oversight of federal information security programs. DPPS has complied with the act by providing DFAS management with all requested information needed to fulfill agency requirements. The DPPS Fiscal Year 2003 Budget Estimate contains the required Government Information Security Reform Act information.

   Estimated Completion Date: Complete. The Program Management Office has reviewed the provisions of the Government Information Security Reform Act and our assessment is that DPPS development and security planning complies with GISRA provisions.

If you have any additional questions or need for clarification, please feel free to contact Mr. Mark E. Easton, DPPS Program Manager, at 614-693-8997 or mark.e.easton@dfas.mil.

Kathleen D. Noe

KATHLEEN D. NOE
Director for Systems Integration
Defense Finance and Accounting Service Arlington

Team Members

The Defense Financial Auditing Service Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Paul J. Granetto
Richard B. Bird
David F. Vincent
Barbara A. Sauls
Yolanda C. Watts
Randall M. Critchlow
Yalonda N. Blizzard
Leon D. Bryant
Ann Thompson