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

May 18, 2007

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER
ASSISTANT SECRETARY OF DEFENSE (NETWORKS AND INFORMATION INTEGRATION)/DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: DFAS Corporate Database/DFAS Corporate Warehouse Compliance with the Defense Business Transformation Certification Criteria (Report No. D-2007-101)

Introduction. We are providing this report for your information and use. No written response to this report was required. Therefore, we are publishing this report in final form.

Background. The Deputy Under Secretary of Defense (Business Transformation) requested that we review DoD Component compliance with the Defense Business Transformation System Certification Criteria. This report is one in a series and discusses compliance of the Defense Finance and Accounting Service (DFAS) Corporate Database/DFAS Corporate Warehouse (DCD/DCW) with the Defense Business Transformation System Certification Criteria. Additional reports will discuss other business systems compliance.

The "Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005" (NDAA) states that funds appropriated for Defense business system modernizations in excess of $1 million may not be obligated unless certified by the Designated Approving Authority and approved by the Defense Business Systems Management Committee. To comply with the NDAA, the Defense Business Systems Management Committee issued the "Investment Review Board Concept of Operations." The Investment Review Board Concept of Operations provides guidance on certifying Defense business system

investments in excess of $1 million, which require review and approval by the Office of the Secretary of Defense (OSD). Defense business system investments under $1 million do not require an OSD-level review and approval, unless designated as a special interest program.* Instead, investments under $1 million are subject to a Component-level review and approval process. Component-level investment review processes should be consistent with the NDAA and the Investment Review Board Concept of Operations.

The Business Transformation Agency (BTA) currently owns DCD/DCW. However, during the time of this audit, DFAS owned the system. DCD/DCW is a Tier 2 system designated as a special interest program. DCD/DCW serves as a centralized repository of consolidated DoD financial information that facilitates the sharing of information among systems, functions, and applications, and with internal and external customers.

Objectives. The overall objective was to determine whether DCD/DCW was properly certified and accredited in accordance with Defense Business Transformation Certification criteria. Specifically, we determined whether DCD/DCW complied with the Investment Review Process.

Scope and Methodology. We performed the audit at DFAS Headquarters in Arlington, Virginia and at DFAS Indianapolis, Indiana. We reviewed the DFAS Investment Review Process used to approve the obligation of funding for FY 2006 DCD/DCW modernization efforts. We interviewed members of the Investment Review Working Group (IRWG), as well as the DCD/DCW system manager. We also obtained and reviewed DFAS Investment Review Process procedures and documentation. Specifically, we reviewed charters, designation letters, the FY 2006 DCD/DCW modernization workbook, and other related documentation.

We reviewed and compared the procedures and documentation we found to the following laws, policies, and DFAS guidance related to the Defense Investment Review Process. Specifically, we reviewed the following:

- Public Law 108-375, "Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005," October 28, 2004;
- Public Law 104-208, "Federal Financial Management Improvement Act ," September 30, 1996;
- Public Law 104-106, "Clinger Cohen Act," February 10, 1996;
- DoD Instruction 5200.4, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997;

* "Special interest" is based on technological complexity, Congressional interest, or program criticality to the achievement of a capability or set of capabilities. Special interest is also based on whether the program is a joint program or whether the resources committed to the program are substantial.

- DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process Application Manual," July 31, 2000;

- "Investment Review Process Overview and Concept of Operations For Investment Review Boards," May 17, 2005;

- "Business Systems Investment Review Proposal Submission Guideline," July 17, 2005; and

- "DoD Information Technology Registry Merger Into the DoD Information Technology Portfolio Registry," September 28, 2005.

We performed this audit from May 17, 2006 through June 16, 2006, in accordance with generally accepted government auditing standards. We postponed the audit due to other priorities and reannounced the audit on March 5, 2007. We did not review the management control program as it related to the Investment Review Process because none has been established for this process.

Results. Our review of the Investment Review Process for DCD/DCW identified three deficiencies. Specifically, DFAS did not have controls in place to ensure segregation of duties when posting the certification package to the DFAS e-Portal and the Investment Review Board (IRB) Portal. In addition, controls were not in place to monitor and track changes made to the certification documentation after posting the package to the DFAS e-Portal and the IRB Portal. Finally, the DCD/DCW Program Office did not obtain the appropriate coordination signatures for the System Security Authorization Agreements (SSAAs) for DCD/webMethods© and DCW/Cognos® before the Designated Approving Authority (DAA) certified the system.

We understand that DCD/DCW transitioned to BTA and is no longer the responsibility of DFAS. However, the DFAS certification submission process should include procedures that maintain segregation of duties when posting certification information to the DFAS e-Portal and the IRB Portal; monitor and track changes made to certification documentation; and ensure that the SSAAs include all coordination signatures prior to DAA approval.

Segregation of Duties. The DCD/DCW Program Office could not maintain segregation of duties when posting the completed certification package to the DFAS e-Portal, as required by the Investment Review Submission guidelines. Specifically, staff in the DFAS Chief Information Officer's (CIO) office posted the certification package information to both the DFAS e-Portal and the IRB Portal. This occurred because the DCD/DCW system manager did not have access to the e-Portal. DFAS implemented the DFAS e-Portal in June 2005, and the DFAS CIO granted DFAS e-Portal access to the DCD/DCW Business Line Portfolio Manager, who initially uploaded the certification information. After DFAS phased out Business Lines in March 2006, the DFAS CIO granted system managers access to the DFAS e-Portal. However, the DFAS CIO had not trained the system managers on the use of the DFAS e-Portal and the deadline for submitting certification information was August 2006. Therefore, to prevent further

delays in submitting the certification documents, the DFAS CIO staff stepped in to upload documents to the DFAS e-Portal until the DFAS CIO could properly train the system managers. To ensure that the integrity of the certification package is preserved, the DCD/DCW Program Office should upload certification information to the DFAS e-Portal, and the DFAS CIO Office should upload certification information to the IRB Portal.

Investment Review Submission guidelines require that the Pre-Certification Authority post business system certification submission documents to the IRB Portal. Likewise, the DFAS CIO requires program managers to post system information to the DFAS e-Portal. DFAS system managers and the DFAS CIO should ensure proper segregation of duties by requiring the DCD/DCW system manager to post the certification submission package to the DFAS e-Portal and requiring the DFAS CIO to post the certification documents to the IRB Portal. Although we identified this discrepancy during the audit, DFAS has since resolved this issue by granting access to the DFAS e-Portal to all system managers in March 2006. The DFAS CIO staff no longer uploads certification documents to the DFAS e-Portal.

Change Controls. Controls were not in place to monitor and track changes made to certification documents posted to the DFAS e-Portal. Specifically, the DCD/DCW Program Office did not maintain a record of changes made to DCD/DCW certification information after it posted the information to the DFAS e-Portal. In addition, controls did not exist to ensure that certification information submitted by the system manager to the Business Line Portfolio Manager and the DFAS CIO staff matched the certification information in the DFAS e-Portal and the IRB Portal. This occurred because the DCD/DCW system manager did not have access to the DFAS e-Portal during the time of submission. The Business Line Portfolio Manager from the DFAS Acquisition Management Office worked with the DCD/DCW system manager and functioned as a coordinator for uploading the certification information to the DFAS e-Portal. Since only the Business Line Portfolio Manager had access to the DFAS e-Portal, the DCD/DCW system manager could not verify that all requested changes reflect in the current version of the certification information in the DFAS e-Portal.

Although the DFAS e-Portal maintains all versions of certification submissions, information may be unintentionally altered without the knowledge of a system manager. Consequently, management may not be able to rely on the certification information. Although we identified this discrepancy during the audit, DFAS has since resolved this issue by granting access to the DFAS e-Portal to all system managers in March 2006.

Coordination Signatures for the SSAAs. DCD/DCW was not in full compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Specifically, the DCD/DCW Program Office did not obtain the coordination signatures on the SSAAs for DCD/webMethods© and DCW/Cognos® before the DAA certified the system. This occurred because DCD/DCW Program Office staff received inaccurate information from the DAA office regarding the requirement for

signatures. As a result of the lack of signature coordination, there was no way to determine whether the SSAA had been properly reviewed. This may compromise the confidentiality, integrity, and availability of the system's data.

The DITSCAP describes the SSAA as a formal agreement among the DAA, certifier, user representative, and program manager. The purpose of the SSAA is to be the basis of agreements throughout the system's life cycle. At each stage of development or modification, more details are added to the SSAA. Any changes in the system that affect its security posture must be submitted to the DAA, certifier, program manager, and user representative for approval and inclusion in a revised SSAA. In order for the SSAA to serve as a reliable, formal agreement, it must be signed by the certifier, user representative, and program manager before it is certified by the DAA. The staff was informed that signatures would be required in the future, but were not necessary at that time. However, while we were on site, the program office obtained the necessary signatures and included them in the current SSAA.

Discussion of Results. We discussed the results of our work with the DCD/DCW Program Office staff. They concurred with our conclusions, and DFAS took action to correct the segregation of duties and change control deficiencies. The program office corrected the coordination of signatures issue during the audit. As a result, this memorandum report contains no recommendations and requires no further action.

We appreciate the courtesies extended to the staff. Questions should be directed to Patricia A. Marsh at (703) 428-1422 (DSN 328-1422) or Donna A. Roberts at (703) 428-1070 (DSN 328-1070).

Paul J. Granetto, CPA
Assistant Inspector General and Director
Defense Financial Auditing Service

cc:

Deputy Under Secretary of Defense for Business Transformation
Director, Acquisition Resource and Analysis