DEFENSE FINANCE AND ACCOUNTING SERVICE

Operational Data Store (ODS)

Unique Project (Investment) Identifier –

007-97-01-01-02-8202-00

PRIVACY IMPACT ASSESSMENT (PIA)

Point of Contact

Reviewing Official

Chief Information Officer (CIO)
DFAS-HT

PREPARED BY

January 23, 2009

PRIVACY IMPACT ASSESSMENT

1. **Department of Defense Component.** Defense Finance and Accounting Service

2. **System Title.** Operational Data Store (ODS)

3. **Budget System Identification Number.** 8202

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).** 13

5. **IT Investment (OMB Circular A-11) Unique Identifier (if applicable).** 007-97-01-01-02-8202-00

6. **Privacy Act System of Records Notice Identifier (if applicable).** T-7900

7. **OMB Information Collection Requirement Number (if applicable) and Expiration Date.** N/A

8. **Type of authority to collect information (statutory or otherwise).**

   5 U.S.C. 301, Departmental Regulations, Department of Defense Financial Management Regulation (DoDFMR) 7000.14R, Vol. 10; 31 U.S.C. Sections 3512 and 3513; and E.O. 9397 (SSN) .

9. **Provide a brief summary or overview of the IT system (activity/purpose, present life cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).**

   a. **Activity/Purpose.**

   To permit DFAS and Army financial managers the ability to retrieve, review and update financial payment information. Database records are also used for extraction or compilation of data and reports for budget execution status and statistical analyses for use internally or externally as required by DoD or other government agencies. System Access & Authorization Request (SAAR) Web module allows electronic collection of user information for access to DFAS systems.

   b. **Present Life Cycle Phase.** Operations & Support.

   c. **System Owner.**

   Defense Finance and Accounting Service.

   d. **System boundaries and interconnections.**

File interfaces are exchanged to or from the following systems:

Entitlement systems:

1. Computerized Accounts Payable System (CAPS).
2. Integrated Automated Travel System (IATS).

Disbursing Systems:

1. Standard Finance System Redesign, Sub-System One (SRD I).
2. Mechanization of Contract Administration System (MOCAS).

Accounting Systems:

1. Standard Army Finance System (STANFINS).
2. Standard Operations and Maintenance, Army R&D System (SOMARDS).
3. Standard Industrial Fund System (SIFS).
4. Command Commodity Standard System (CCSS).
5. Corp of Engineer Financial Management System (CEFMS).
6. Logistics Modernization Program (LMP).

Logistic Systems:

1. Army Food Management Information System (AFMIS).
2. Fuels Automated System (FAS).
3. Theater Army Medical Management Information System (TAMMIS).
4. Defense Medical Logistics Support Service (DMLSS).
5. Defense Automatic Addressing System Center (DAASC).
6. TAMMIS Enterprise Wide Logistics System (TEWLS).
7. Funds Control Module (FCM).

Pay Systems:

1. Defense Joint Military Pay System – Active Component (DJMS-AC).
2. Defense Joint Military Pay System – Reserve Component (DJMS-RC).
3. Defense Civilian Pay System (DCPS).

Other Systems:

1. Defense Integrated Financial System (DIFS).
2. Centralized Integrated System-International Logistics (CISIL).
3. Program Budget Accounting System (PBAS).
4. Defense Cash Accountability System (DCAS).
5. Automated Fund Control Order System (AFCOS).
6. Army Shared Knowledge – Financial Management (ASK-FM)
7. Corporate Electronic Funds Transfer Database (CEFT).
8. Headquarters Accounting and Reporting System (HQARS).
9. Resource Mapping Tool (RMT).
10. Installation Management Agency (IMA).
11. Business Enterprise Information System (BEIS).
12. Defense Corporate Warehouse (DCW).
13. Comptroller's Accounting and Budget System (CABS).
14. Financial Accounting and Corporate Tracking System (FACTS)/Financial Management Solution (FMS) for the National Security Agency (FACTS/FMS).
15. SAAR Web Module (ODS).

e. **System Location and Components.**

System hardware is located at Defense Information Systems Agency (DISA) Ogden, UT.

f. **System Backup.**

Alternate site is located at DISA St. Louis, MO.

10. **Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)**

a. **Information in Identifiable Form.**

Individual name, home address, Social Security Number (SSN), and tax identification number.

b. **DFAS IT systems.**

Commercial Accounts Payable (CAPS), Defense Civilian Payroll System (DCPS), Integrated Automated Travel System (IATS), Defense Joint Military Pay System – Active Component (DJMS-AC), Defense Joint Military Pay System – Reserve Component (DJMS-RC) and SAAR Web module (ODS).

c. **DoD Component IT systems.**

N/A

d. **IT systems from agencies outside DoD.**

N/A

11. **Describe how the information will be collected (e.g. via the Web, via paper-based collection, etc.)**

ODS only receives the information in the form of an electronic interface file produced by the entitlement systems referenced in paragraph 10b. ODS doesn't collect from the public and report the information in identifiable form.

12. **Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.)**

Information is necessary for mandatory reports to the US Treasury and to generate payments to individuals based upon system edits.

13. **Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.)**

(a) ODS uses the information to permit DFAS and Army financial managers the ability to retrieve, review and update financial payment information. The information is also used for archive requirements and to support litigation and audit requirements.

(b) The DoD "Blanket Routine Uses" apply to this system of records.

14. **Describe whether the system derives or creates new data about individuals through aggregation.**

ODS does not derive or create new data about individuals through aggregation.

15. **Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.)**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(a) The information will be used by Federal, State, and local agencies for the purpose of conducting computer matching programs regulated by the Privacy Act of 1974, as amended, (5 U.S.C. 552a). The information will be used to generate payments for accounts receivable and for financial reporting.

(b) The DoD "Blanket Routine Uses" apply to this system of records.

16. **Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.**

DFAS entitlement systems and the SAAR Web module of ODS collect the data and a Privacy Act Statement is provided when the personal data is collected. The individuals are informed in the statement that providing the data is voluntary, and it allows the individuals the opportunity to object to collection of information.

17. **Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.**

The DFAS Entitlement systems collect the personal data with forms that contain the Privacy Act statement, and SAAR Web module of ODS electronically collects personal information directly from the individual and provides Privacy Act Statement.

18. **Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form**

Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for a need-to-know. Passwords and digital signatures are used to control access to the system data, and procedures are in place to deter and detect browsing and unauthorized access.

19. **Identify whether the IT system or collection of information will require a System of Records(SOR) notice as defined by the Privacy Act of 1974, and as implemented by DoD Directive 5400.11-R, "DoD Privacy Program," November 11, 2004. If so, and a SOR notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.**

A Privacy Act systems notice has been published in the Federal Register, 71 FR 42357, on July 26, 2006.

20. a. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form.**
b. **Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals.**
c. **Describe/evaluate any privacy risks posed by the adopted security measures.**

There are no identified risks posed by the adopted security measures at this time. Security controls are reviewed annually and the system is recertified and reaccredited at least every three years. Risks are evaluated and mitigated whenever they are discovered or identified.

21. **State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.**

ODS is classified as sensitive, for official use only. Yes, PIA should be published in full form.

SIGNATURE PAGE - ODS

Preparing Official
Name:
Title: System Manager, ODS
Organization: Defense Finance and Accounting Service, Accounting Systems
Work Phone Number: 317-510-7283
E-mail:

Jan 23, 2009
date

Information Assurance Officia
Name:
Title: Director, CIO Oversight
Organization: Defense Finance and Accounting Service, Information and Technology
Work Phone Number: (703) 607-5014
E-mail:

Mar 3, 2009
date

Privacy Officer
Name:
Title: Freedom of Information/Privacy Act Program Manager
Organization: Defense Finance and Accounting Service, Corporate Communications and Legislative Liaison (DFAS-HAC/Denver)
Work Phone Number: (303) ~~676-6046~~ 589-3510
E-mail:

1/23/09
date

Reviewing Official
Name:
Title: Director, Information and Technology
Organization: Defense Finance and Accounting Service, Information and Technology Directorate (DFAS-HT)
Work Phone Number: (703) 607-0328
E-mail:

3/3/09
date