DEFENSE FINANCE AND ACCOUNTING SERVICE

Resume Retrieval Application

IT Investment Unique Identifier – N/A

PRIVACY IMPACT ASSESSMENT (PIA)

Point of Contact

[redacted]

HR Specialist

Component Reviewing Official

[redacted]

Chief Information Officer

Prepared by

[redacted]

January 2007

Unclassified

DOD Privacy Impact Assessment for Resume Retrieval Application

1. Department of Defense Component. Defense Finance and Accounting Service (DFAS)

2. Name of Information Technology System. Resume Retrieval Application (RRA)

3. Budget System Identification Number. N/A

4. System Identification Number. Not assigned.

5. IT Investment Unique Identifier. N/A

6. Privacy Act System of Records Notice Identifier. OPM/GOVT-5

7. OMB Information Collection Requirement Number and Expiration Date. Office of Management and Budget (OMB) 3206-0219, Optional Form (OF) 612

8. Type of authority to collect information.

   DFAS rates applicants for Federal jobs under the authority of 5 United States Code, sections 1104, 1302, 3301, 3304, 3320, 3361, 3393, 3394. DFAS needs the information requested on the resume form regarding an associated vacancy announcement to evaluate a job applicant's qualifications. Other laws require DFAS to ask about citizenship, military service, etc. DFAS requests an applicant's Social Security Number (SSN) under the authority of Executive Order 9397 in order to uniquely identify applicants.

9. Overview of the IT system.

   This system's purpose is to collect information from job applicants in a resume format. The system is fully operational and is in the maintenance phase of its life cycle. The DFAS Strategic Business Management Directorate, Human Resource (HR) Office manages this system. Job applicants enter information into the system through an online resume builder. The system then exports this information to Resumix, for use by HR specialists in determining qualifications and rankings. The system is physically located at the Defense Information Systems Agency (DISA)/Defense Enterprise Computing Center (DECC), 450 Duncan Drive, San Antonio, TX 78226-1834.

10. Information that will be collected.

    Personal information will be collected which will include, but is not limited to, name, address, phone number, social security number, gender, race, disability, veteran's preference, education, work history, salary history, training history, and award history.

11. Methods of collecting information.

The information will be collected using a secure Web site at www.dod.mil/dfas. DFAS may also accept an extremely limited number of resumes submitted on paper or 3.5" disk.

12. Reasons for collecting information.

Without the necessary information, DFAS managers and HR specialists will not have a rational basis for making appointment, promotion, change to lower grade, reassignment, detail, and transfer decisions.

13. How information collected will be used.

The information collected will be used to make personnel decisions within DFAS to include appointments, promotions, change to lower grade, reassignments, details, and transfers.

14. Deriving or creating new data through aggregation.

The resume retrieval application does not derive or create new data through aggregation. However, the systems that the resume retrieval application interacts with may aggregate non-personally identifiable data for statistical or reporting purposes.

15. Sharing of identifiable information.

Personally identifiable information (PII) will be shared with DFAS managers, supervisors, HR specialists, and Equal Employment Opportunity (EEO) specialists. Members of selection committees may also see resumes that contain personally identifiable information. See Office of Personnel Management (OPM) Privacy Act system of records notice OPM/GOVT-5, for full details on who this information may be shared with other than DFAS employees. The Privacy Act system of records notice is published at the following Web site: http://www.dod.mil/privacy/govwide/opm_govt-5.html

16. Objecting to collection of identifiable information.

Job applicants can object to providing PII by refusing to answer a question on the DFAS resume builder. However, if an applicant does this, they may lose consideration for a job that they applied for with DFAS.

17. Information and format of information provided to individuals.

Job applicants and potential job applicants have access to a Privacy Act statement that is available electronically at the following website:
http://www.dod.mil/dfas/careers/post/privacyactstatement.html
If the applicant uses an OF 614 to submit their resume, the form contains a Privacy Act Statement.

18. Preserving confidential information.

Connections between the job applicant's web browser and the Resume Retrieval Application are encrypted using Secure Sockets Layer (SSL). All DISA, DECC, San Antonio personnel that have unescorted access to the Resume Retrieval Application, Oracle Database, and Resumix programs must have a Secret security clearance. All DFAS HR personnel have successfully passed a background investigation and can view noncritical-sensitive data, such as personnel data. Physical access to the DISA/DECC San Antonio facility and to the DFAS Indianapolis facility are controlled by armed guards who inspect DoD issued identification cards. Physical access to other DFAS facilities may be controlled by a combination of armed guards, DoD issued identification cards, keys, or other equivalent measures. DISA/DECC, and DFAS business rules are in place to ensure that only individuals with a "need-to-know" will be given access to personally identifiable information. System auditing and monitoring is used to detect any attacks on the system or misuse of the system. DISA/DECC maintains backup files of the Oracle database that houses job applications and resumes. DISA/DECC has a redundant power supply for all their computer systems.

19. System of Records Notice

The OPM/GOVT-5 applies to this system of records.

20. Potential privacy risks.

There are no privacy risks in letting individuals object or consent to providing DFAS PII. There are no privacy risks in the collection of PII, but there are privacy risks in its use. DISA/DECC, and DFAS employees with access to PII could commit fraud with that information, disclose that information without authorization, or fail to protect access to that information. These risks are mitigated by the security measures discussed in #18 above.

21. Classification of system

The system is unclassified. The PIA should be published in full form.

SIGNATURE PAGE FOR RRA PIA

Preparing Official ____Electronically Signed: [redacted] ____1/26/2007_____
Name: [redacted] **date**
Title: HR Specialist
Organization: Defense Finance and Accounting Service
Work Phone Number: [redacted]
Email: [redacted]

Information Assurance Official _____ [redacted] _____1/26/07
Name: [redacted] **date**
Title: Acting Division Manager
Organization: DFAS Information and Technology Directorate/Strategic Architecture & Information Assurance
Work Phone Number: [redacted]
E-mail: [redacted]

Privacy Officer [redacted] _____1/26/07
Name: Linda K[redacted] **date**
Title: Freedom of Information/Privacy Act Program Manager
Organization: Defense Finance and Accounting Service, Corporate Communications and Legislative Liaison
DFAS-HAC/DE
Work Phone Number: [redacted]
E-mail: [redacted]

Reviewing Official [redacted] _____1/26/2007
Name: [redacted] **date**
for **Chief Information Officer**
Organization: Defense Finance and Accounting Service, Information and Technology Directorate (DFAS-DT/HQ)
Work Phone Number: [redacted]
E-mail: [redacted]