DoD Privacy Impact Assessment (PIA)

1. Department of Defense (DoD) Component.

United States Air Force (USAF)

2. Name of Information Technology (IT) System.

Air Force Recruiting Information Support System – Reserve (AFRISS-R)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

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

1754

5. IT Investment (Office of Management and Budget (OMB) Circular A-11) Unique Identifier (if applicable).

Not Applicable.

6. Privacy Act System of Records Notice (SORN) Identifier (if applicable).

A SORN is expected to be published in the Federal Register by 2009.

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

- Department of Defense (DD) Form 1966/1, March 2007 - Record of Military Processing - Armed Forces of the United States - Office of Management and Budget (OMB) No. 0704-0173, OMB approval expires March 31, 2010

- DD Form 2807-2, March 2007 - Medical Prescreen of Medical History Report
 - OMB No. 0704-0413, OMB approval expires March 31, 2010

- Standard Form 180, Rev. 4-07 - Request Pertaining to Military Records - OMB No. 3095-0029, Expires 9/30/2008

- Standard Form 86, Revised September 1995 - Questionnaire for National Security Positions - OMB No. 3206-0007, ICR Reference No: 199804-3206-005, 02/28/2002

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

- Title 10, United States Code (U.S.C.) Subtitle E Section 10202 - Armed Forces, Reserve Components, Organization and Administration, Administration of Reserve Components, Regulations

- Title 10, U.S.C. Subtitle E Section 10205 - Armed Forces, Reserve Components, Organization and Administration, Administration of Reserve Components, Members of Ready Reserve: requirement of notification of change of status

- Title 10, U.S.C. Subtitle E Section 10174 - Armed Forces, Reserve Components, Organization and Administration, Reserve Component Commands, Air Force Reserve Command

- Title 10, U.S.C. Subtitle E Section 10110 - Armed Forces, Reserve Components, Organization and Administration, Reserve Components Generally, Air Force Reserve: composition

- Air Force Policy Directive (AFPD) 36-20, Accession of Air Force Military Personnel

- Air Force Instruction (AFI) 36-2115, Assignments within the Reserve Components

- Executive Order (EO) 9397 (Social Security Number - SSN)

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

AFRISS-R provides Air Force Reserve Command Recruiting Service (AFRCRS) recruiters with a recruiting automation system that meets the distinct set of required features essential for AFRCRS to meet mission objectives. The system gives AFRCRS management personnel the tools needed to better respond to and guide the recruiting environment and process.

Present lifecycle phase is Operational/maintenance.

The hardware, software application, and data are owned and maintained by Headquarters Air Force Reserve Command, Recruiting Service (HQ AFRC/RS).

The system boundaries/interconnections are the AFRC Enterprise Network, Blaine-Warren Advertising Agency, United States Military Entrance Processing Command (USMEPCOM), Military Entrance Processing Station (MEPS) Information Reporting System (MIRS), Defense Security System (DSS) Joint Personnel Adjudication System (JPAS), and the Air Force Recruiting Information Support System (AFRISS).

The core resources are located in the AFRC Network Operations and Security Center (NOSC) at Robins Air Force Base (AFB), Georgia (GA).

Backups are also maintained.

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 Department of Defense (DoD), etc.).

Name, Social Security Number, marital status, name of dependents, number of dependents, sex of dependents, address, telephone number, civilian educational degrees and major areas of study, school and year of graduation, home of record, age and date of birth, present assignment, race/ethnic origin and educational level. Information is user disclosed.

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

Information gathered is both paper-based and electronic.

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.).

The information is collected to facilitate execution of the AFRC recruiting program. The information collected is the minimum required in executing the AFRC recruiting mission.

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

Information will be used to determine basic eligibility for Reserve accession.

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

Examples of AFRISS-R derived data are as follows: Applicant qualification for accession in the Air Force Reserve; applicant qualification for Air Force Specialty Code selection in the best interest of the Air Force Reserve; and security clearance eligibility, qualification, or validation.

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.).

The information in identifiable form will be shared with the Blaine-Warren Advertising Agency, USMEPCOM/MIRS, DSS/JPAS, and AFRISS.

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.

The requester shows and, upon request, gives the affected individual a Privacy Act Statement for each form, format, or form letter used to collect personal data before asking for the information. Individual signatures grant consent.

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 requester shows and, upon request, gives the affected individual a Privacy Act Statement for each form, format, or form letter used to collect personal data before asking for the information. The statement is delivered in written format.

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.

18.1. The PIA is based on proper implementation, validation, and verification of the baseline information assurance controls for CONFIDENTIALITY in accordance with Department of Defense Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation*. The controls address the administrative, physical, and technical controls required to secure, protect, and preserve the confidentiality of information in identifiable form.

18.2. AFRISS-R is a mission assurance category (MAC) III system with a confidentiality level of "Sensitive." AFRISS-R is fully certified and accredited and has implemented/validated the DoDI 8500.2 baseline controls for systems with a confidentiality level of "**SENSITIVE.**"

Baseline IA controls validated for AFRISS-R:

EBBD-2	Boundary Defense
EBPW-1	Public Wide Area Network Connection
EBRP-1	Remote Access for Privileged Functions
EBRU-1	Remote Access for User Functions
ECAD-1	Affiliation Display
ECAR-2	Audit Record Content – Sensitive Systems
ECAT-1	Audit Trail, Monitoring, Analysis, and Reporting
ECCR-1	Encryption for Confidentiality (Data at Rest)
ECCT-1	Encryption for Confidentiality (Data at Transmit)
ECIC-1	Interconnections among DoD Systems and Enclaves
ECLO-1	Logon
ECLP-1	Least Privilege
ECML-1	Marking and Labeling
ECMT-1	Conformance Monitoring and Testing

ECNK-1	Encryption for Need-to-Know
ECRC-1	Resource Control
ECRR-1	Audit Record Retention
ECTC-1	Tempest Controls
ECWM-1	Warning Message
IAAC-1	Account Control
IAGA-1	Group Identification and Authentication
IAIA-1	Individual Identification and Authentication
PRAS-1	Access to Information
PRMP-1	Maintenance Personnel
PRNK-1	Access to Need-to-Know Information
PRTN-1	Information Assurance Training
PECF-1	Access to Computing Facilities
PECS-1	Clearing and Sanitizing
PEDI-1	Data Interception
PEPF-1	Physical Protection of Facilities
PEPS-1	Physical Security Testing
PESP-1	Workplace Security Procedures
PESS-1	Storage
PEVC-1	Visitor Control to Computing Facilities
DCAS-1	Acquisition Standards
DCSR-2	Specified Robustness – Medium

SORN Review: A SORN is expected to be published in the Federal Register by 2009.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, DoD Privacy Program, May 8, 2007; and DoD 5400.11-R, Department of Defense Privacy Program, May 14, 2007. If so, and a System 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 SORN is expected to be published in the Federal Register by 2009.

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

There are no identifiable risks to report.

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.

Unclassified. This PIA will be published in full.

Privacy Impact Assessment Approval Page for ___AFRISS-R_____

Preparing Official ████████████_____ (Signature) _5 May 08_ (Date)
Name: ████████████
Title: MSgt
Organization: AFRC/RSAI
Work Telephone Number: ████████████
E-mail: ████████████

Information Assurance Official ████████ (Signature) _6/2/08_ (Date)
Name: ████████
Title: Civ
Organization: AFRC/A6II
Work Telephone Number: ████████
E-mail: ████████

MAJCOM Privacy Act Official ████████ (Signature) _6/3/08_ (Date)
Name: ████████
Title: Civ
Organization: HQ AFRC/A6IE (PA)
Work Telephone Number: ████████
E-mail: ████████

HQ Air Force Information Assurance Official ████ (Signature) _15 Aug 08_ (Date)
Name: ████████
Title: Information Assurance Officer
Organization: SAF/XCPPI
Work Telephone Number: ████████
E-mail: ████████

HQ Air Force Privacy Act Officer ████████ (Signature) _8/25/08_ (Date)
Name: ████████
Title: Air Force Privacy Act Officer
Organization: SAF/XCPPI
Work Telephone Number: ████████
E-mail: ████████

Reviewing Official ████████████ (Signature) _12 Sep 08_ (Date)
Name: ████████
Title: Air Force Chief Information Officer
Organization: SAF/XC, Office of Warfighting Integration and Chief Information Officer
Work Telephone Number: ████████
E-mail: ████████

PIA For AFRISS-R