DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement on a New System of Records
Under the Privacy Act of 1974

1. System identifier and name: DPA 02, entitled "AFNConnect (AFNC)".

2. Responsible official: Mr. Carl O'Day, Application Development and Support Manager, Defense Media Activity, 23755 Z Street, Riverside, CA 92518-2077; telephone: 951-413-2569.

3. Purpose of establishing the system: The Office of the Secretary of Defense proposes to establish a new system of records which will document the eligibility and continued validation of authorized individuals outside the Continental United States (OCONUS) who register an American Forces Network satellite decoder. AFNConnect provides U.S. military commanders worldwide a means to communicate internal information to OCONUS users. Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

4. Authority for the maintenance of the system: 10 U.S.C. 113, Secretary of Defense, DoD Directive (DoDD) 5122.05, Assistant Secretary of Defense for Public Affairs; DoDD 5105.74, Defense Media Activity; and DoD Instruction 5120.20, American Forces Radio and Television Service (AFRTS).

5. Provide the agency's evaluation on the probable or potential effects on the privacy of individuals: In developing this system of records notice, The Defense Media Activity (DMA) carefully reviewed the safeguards established for the system to ensure they are compliant with DoD requirements and are appropriate to the sensitivity of the information stored within this system. Any specific routine uses have been established to ensure the minimum amount of personally identifiable information is provided.

6. Is the system, in whole or in part, being maintained, collected, used or disseminated by a contractor? No.

7. Steps taken to minimize risk of unauthorized access: Records are accessible only to personnel on a need-to-know basis to perform their duties. All records are maintained on a protected network. Access to the network where records are maintained requires a valid Common Access Card (CAC). Electronic files and databases are password protected with access restricted to authorized users and networks. Access to physical hardware

(i.e. webservers, database servers) is controlled via electronic key lock and is monitored by closed circuit TV. All data transferred via web technologies is protected via industry standard Secure Socket Layer encryption.

8. Routine use compatibility: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the Department of State to verify authorized personnel's use of an AFN satellite.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Disclosures Required by International Agreements Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

9. OMB information collection requirements:
OMB collection required: Yes.
OMB Control Number:
Title of collection if other than #10:
Date Approved or Submitted:
Expiration Date:

Provide titles of any information collection requests (e.g., forms and number, surveys, etc.) contained in the systems of records:

If collecting on members of the public and/or no OMB approval is required; state the applicable exception(s):

10. Name of IT system (state NONE if paper records only):
American Forces Network – Broadcast Center; DITPR #15409.

DPA 02

System name:
AFNConnect (AFNC)

System location:
American Forces Network – Broadcast Center (AFN-BC), 23755 Z Street, Riverside, CA 92518-2077.

Categories of individuals covered by the system:
Eligible military personnel (including retirees and reservists), DoD civilian employees, full time direct hire Department of State (DoS) employees, DoD contractors, and their OCONUS family members, to include widows, maintaining an AFN satellite decoder.

Categories of records in the system:
First and last name, duty station/residence country and locality, Unit Identification Code (UIC), DoD ID Number, sponsor/dependent status, home telephone number, address,
personal cell phone number, office telephone number, grade/rank, date of birth, organization assigned to (i.e., Department, directorate, branch, office), status (i.e., active duty, retired, or permanently disabled) and decoder serial number.

Authority for maintaining the system:
10 U.S.C. 113, Secretary of Defense, DoD Directive (DoDD) 5122.05, Assistant Secretary of Defense for Public Affairs; DoDD 5105.74, Defense Media Activity; and DoD Instruction 5120.20, American Forces Radio and Television Service (AFRTS).

Purpose(s):
To document the eligibility and continued validation of authorized individuals outside the Continental United States (OCONUS) who register an AFN satellite decoder. AFNConnect provides U.S. military commanders worldwide a means to communicate internal information to OCONUS users. Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

Routine uses of the system records, including categories of users and their purpose for using the system:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the Department of State to verify authorized personnel's use of an AFN satellite.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Disclosures Required by International Agreements Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed

to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Electronic storage media.

Retrievability:
Records are retrieved by various combinations of name, e-mail address, location, date of birth, and/or decoder serial number.

Safeguards:
Records are accessible only to personnel on a need-to-know basis to perform their duties. All records are maintained on a protected network. Access to the network where records are maintained requires a valid Common Access Card (CAC). Electronic files and databases are password protected with access restricted to authorized users and networks. Access to physical hardware (i.e. webservers, database servers) is controlled via electronic key lock and is monitored by closed circuit TV. All data transferred via web technologies is encrypted in transit and at rest.

Retention and disposal:
Inactive records are destroyed/deleted six (6) years after user account or access is terminated.

System manager(s) name and address:
Director, American Forces Radio and Television Service, Defense Media Activity, 6700 Taylor Avenue, Fort Meade, Maryland 20755-7061.

Director, AFN-BC, Defense Media Activity, 23755 Z Street, Riverside, California 92518-2077.

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Privacy Act Officer, Defense Media Activity, 6700 Taylor Avenue, Fort Meade, Maryland 20755-7061.

Signed, written requests should contain name, duty station address, and home or office phone number for positive identification of requester.

Record access procedures:
Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington DC 20301-1155.

Signed, written requests should contain name, home address and phone number for positive identification of requester and the name and number of this system of records notice.

Contesting record procedures:
The Office of the Secretary of Defense (OSD) rules for accessing records, for contesting content, and appealing initial agency determinations are contained in OSD Administrative Instruction 81, 32 CFR part 311, or may be obtained from the system manager.

Record source categories:
Individual and Defense Enrollment Eligibility Reporting System (DEERS).

Exemptions Claimed for the System:
None.