



PRIVACY IMPACT ASSESSMENT (PIA)

For the

American Forces Network - Broadcast Center
Defense Media Activity - Riverside

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- ☐ (1) Yes, from members of the general public.
- ☐ (2) Yes, from Federal personnel* and/or Federal contractors.
- ☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- ☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ New DoD Information System ☐ New Electronic Collection
- ☒ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ Yes, DITPR Enter DITPR System Identification Number
- ☐ Yes, SIPRNET Enter SIPRNET Identification Number
- ☐ No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ Yes ☒ No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ Yes ☐ No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number

In process

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 113, Secretary of Defense, DoDD 5122.05, Assistant Secretary of Defense for Public Affairs; DoDI 5120.20, American Forces Radio and Television Service (AFRTS); and DoDD 5105.74, Defense Media Activity.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To determine the eligibility and continued validation of authorized individuals Outside the Continental United States (OCONUS) who receive and utilize an AFN satellite decoder. Provide U.S. military commanders worldwide with a unique means to communicate internal information directly as needed to OCONUS users. Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

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.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

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.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify.

Application developers programming AFNConnect, internal users administering AFNConnect, and DMA HQ personnel with a need for access.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes**

☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Taking advantage of AFN services is voluntary. However, without receiving sufficient data to determine viewer/listener eligibility AFN will decline access to radio and television services via satellite delivery.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes**

☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Information in AFNConnect is used to determine eligibility to receive AFN, demonstrate continued eligibility to receive AFN, to administer the satellite decoder and streaming systems, and to maintain and improve services within financial constraints. These uses are vital to AFN's ability to safeguard content and continue to operate effectively. Taking advantage of AFN services is voluntary and if a user objects to the use of their data for the purposes outlined in this document, they will not be eligible to receive AFN services.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- ☒ Privacy Act Statement
- ☐ Privacy Advisory
- ☐ Other
- ☐ None

Describe each applicable format.

AUTHORITY: 10 USC, 113, DoDD 5122.05, DoDD 5105.74, DoD Instruction 5120.20.

PRINCIPAL PURPOSE: To determine the eligibility and continued validation of authorized individuals Outside the Continental United States (OCONUS) who receive and utilize an American Forces Network (AFN) satellite decoder. Provide U.S. military commanders worldwide with a unique means to communicate internal information directly as needed to OCONUS users. 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.

ROUTINE USE: (a)Truncated SSN/DOB for integration with DEERS for eligibility screening (the truncated SSN is not stored). Remaining Data: Verification of eligibility to receive AFN content, maintain demographic data on AFN's viewership, and increase Force Protection capabilities of local and COCOM commanders. (b) Information can be used by the Department of State to verify authorized personnel's use of an AFN satellite (c) general request for information under the Freedom of Information Act, (d) legitimate request from law enforcement, (e) Congressional Inquiries, (f) Department of Justice for litigation purposes, (g) National Archives and Records Administration (NARA) for the purpose of records management inspections, and (h) disclosures required by International agreement.

DISCLOSURE IS VOLUNTARY: Taking advantage of AFN services is voluntary. However, without receiving sufficient data to determine viewer/listener eligibility AFN will deny access to radio and television services via satellite delivery.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.