

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Fitness Access (AFSV-FA)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

04/05/24

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

☐ From members of the general public

☐ From Federal employees

☒ from both members of the general public and Federal employees

☐ Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

☐ New DoD Information System

☐ New Electronic Collection

☒ Existing DoD Information System

☐ Existing Electronic Collection

☐ Significantly Modified DoD Information System

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

Air Force Services Center Fitness Center Access is considered a Business Mission Area (BMA) system. The AFSV-FA system is the result of the need for global Force Support Squadrons to deliver 24/7 building/IT-based access to fitness centers for authorized patrons. AFSV-FA is provided by SmartNet, using commercial-off -the-shelf (COTS) software and a Non-appropriated Fund Instrumentality (NAFI) contract for a stand-a-lone, non-networked configuration information system (IS). In 2018, the Department of Defense (DOD) approved \$2.6M for AFSV-FA upgrades at 75 global locations including upgrade/sustainment support for system cyber-security. AFSV-FA satisfies DOD-mandated physical and information technology (IT), security, patron safety measures and compensation for extended duty hours at global fitness facilities with additional \$1.9M support that was added. AFSV-FA will be assessed/authorized under Department of Defense Instruction (DoDI) 8500.01 & Air Force Instruction (AFI) 17-101, para 2.6. In 2020 Air Force cyber officials transferred Approving Authority (AO) duties from the HQ AF-A4S boundary to the HQ AF-A1 Boundary with an approval to operate with Conditions with Approving Authority in HQ ACC A6IO per COVID-19 operations. Program Management Office (PMO) is HQ AFMC, AFSVC/SVO. Information technology portfolio is HQ AFMC AFSVC. System is not a National Security System (NSS). System supports over 10K+ personnel globally. System has 1 contract administrator and a local Information System Security Officer (ISSO), and 3 subordinate operators. Contract maintenance and sustainment is by NAFI: (SmartNet), who manages configuration at each installation, with maintenance occurring on site per NAFI contract administered through AFSVC/SVC with oversight from the Mission Owner (MO): AFSVC/CC.

Information Gathered: : Home, Cell or Duty Telephone Number, Official Duty or Personal Email Address, Unique System ID, First Name, Middle Initial, Last Name.

AFSV-FA is an IS as defined by DoDI 8500 and 8510 for global fitness centers supporting registration and beyond normal duty hour patronage. AFSV-FA uses COTS software designed to support the AFSVC NAF patronage for fitness entrance and usage. AFSV-FA IS support is provided via NAFI federal contract with SmartNet Gov.com (WBE, WOSB/EDWOSB), 211 Edwards Ferry Road NE, Leesburg, VA 20176 Tel 703.779.7678 ext. 338. AFSV-FA is stand-alone and non-networked, and is classified as a type-assessment under DoDI 8500 and 8510. The categorization of data collected verbally from a patron acts as the initial collection of PII culminating in IS registration, which results in data storage and processing retrievable by name data elements or a unique system identifier based on data collection. Data collection in the system consists of: Home/Cell Phone, Work E-mail Address, Official Duty Telephone Phone, Personal E-mail Address, Name(s)(i.e. First Name,Middle Initial,Last Name) and Other ID Number (i.e. Unique System ID). All AFSV-FA resources (i.e. hardware, software, and data) are housed in a secure environmentally controlled facility (local fitness center) located at each installation world-wide. Initial information collection is via customer verbally. Data is Low PII, FOUO, Unclassified.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII collection is for verification, authentication and administrative for NAFI mission-related use. AFSV-FA system users must abide by Public Law 93-579, 5 USC 552a, 93rd Congress, S. 3418, The Privacy Act and Department of Defense (DoD) Directive 5400.11, DoD Privacy Program concerning the protection of Privacy Act information. Failure to comply may lead to administrative actions being taken. The purpose for collection is to verify the individual's identification and eligibility to access the local fitness facility beyond normal duty hours as outlined in AFI 34-266, Fitness, Sports, and Worldclass Athlete Program, para 3.1.3.3.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

At the point of initial collection, patrons can opt-out of providing required information. Patrons who opt-out can not receive service. Personal data collected is voluntarily given by the authorized patron of the fitness facility verbally at each installation. The patron is allowed to make an informed decision about providing data as required by 5 U.S.C. 552a(e)(3). The attendant advises the individual that the information provided is voluntary and provides consequences of choosing not to participate with the information collection process. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable or during the data collection). The authorized patron of the fitness facility initiates the collection request and maintenance of his/her information for the purpose of providing information to the fitness facility to gain access to the building after normal operating hours. Authorized patrons of the fitness facility may object to the collection of their PII, but then will not be granted access to use the fitness facility beyond normal duty hours.

f. 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.

At the point of initial collection, patrons are provided an opportunity to verbally consent. At this point, patrons can agree or disagree. Failing to consent, patrons will not receive service.

Personal data collected is voluntarily and verbally given by the authorized patron of the fitness facility at each Fitness Facility, at each installation. As required by 5 U.S.C. 552a(e)(3), the patron can make an informed decision about providing the data. The attendant advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable or during the data collection). The authorized patron of the fitness facility initiates the collection request and maintenance of his/her information for the purpose of providing information to the fitness facility manager to gain access to the facility after normal operating hours. Authorized patrons of the fitness facility may object to the collection of their PII, and if an objection is made, the patron will not be granted access to use the fitness facility beyond normal duty hours. All authorized patrons of the fitness facility agrees in order to participate in the after duty hours access program for the installation fitness center. If patrons want to access the facility after hours of operation, they are advised that the data collection is the minimum data that must be collected that would facilitate data entry into the building and is to support the registration process, which then allows patron access when data is entered into AFSV-FA. Patrons are advised that the data in whole must be collected so that access can be granted. To ensure access, patrons are advised that verbal consent is needed for the the collection and usage of their data for system and procedure processing, in whole, rather than in part, then access is granted to the facility after hours.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

The attendant verbally that explains the purpose and the disposition of the data collected. It also explains the possible results of the failure to provide the requested information, to wit:

Purpose: For managing and delivering a system of quality, available and affordable program and services to assist DoD military and civilian personnel, who are patrons of the United States Air Force Fitness Centers. To obtain personal information, to track usage of the fitness facility after hours of daily operation have terminated.

Authority: 10 U.S.C. 8013, Secretary of the Air Force; implemented by AFI 34-266, Fitness, Sports, and Worldclass Athlete Program, para 3.1.3.3.

Routine Use: 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 be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To medical personnel (military or civilian) in the course of providing the emergency medical attention of a patron enrolled in this program.

To Federal, state, and local officials involved in Fitness Center Services for the purpose of reporting suspected or actual abuse or assault investigations.

To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

SORN: F034 AFPC B

Mandatory or Voluntary Disclosure: Voluntary, Individuals who fail to provide required information will be denied services.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component?
(Check all that apply)

☒ Within the DoD Component

Specify.

At each Fitness Facility globally at each Air Force installation globally, on an individual facility basis only

☐ Other DoD Components (i.e. Army, Navy, Air Force)

Specify.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify.

☐ State and Local Agencies

Specify.

☒ Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

SmartNet Gov.com (WBE, WOSB/EDWOSB), 211 Edwards Ferry Road NE, Leesburg, VA 20176 Tel 703.779.7678 ext. 338. using AFI 33-332.

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

Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

☒ Individuals

☐ Databases

☐ Existing DoD Information Systems

☐ Commercial Systems

☐ Other Federal Information Systems

Source is the physical patron who verbally shares the data required with the attendant. The data is manually entered into the AFSV-FA system.

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- | | |
|---|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input checked="" type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

Data is collected face-to-face at each fitness facility at each installation on a global basis. Data is collected verbally from the patron and entered into AFSV-FA system.

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

NA

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

T 31 - 01 R 21.00 - Entry Control Files - Destroy 2 years after final entry or 2 years after date of document, as appropriate.

T 31 - 04 R 14.00 - Access Control Records - Destroy when superseded, obsolete, or no longer needed.

T 31 - 08 R 05.00 - Limited Access Authorizations at Issuing Authorities - Destroy 2 years after limited access is terminated.

Note 1: Among the dispositions cited in this field, the one with the longest retention time will be used on the system's records data.

Note 2: If any disposition cited in this field has a pending or unscheduled disposition, treat records as permanent retention until an approved NARA disposition is published."

Note 3: If any disposition cited in this field have a permanent retention, retain the records, and prepare for transfer to NARA as scheduled."

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
 - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 8013, Secretary of the Air Force; implemented by AFI 34-266, Fitness, Sports, and Worldclass Athlete Program, para 3.1.3.3.

3.1.3.3. Fitness Access, an Air Force initiative to provide facility access outside of normal operating hours, can be implemented at main, additional, or satellite Force Support fitness facilities. Fitness Access was originally developed for installations with a high number of military shift workers to maintain mission readiness. Installation Commanders or designee must conduct an operational risk management assessment and determine if access will be restricted to specific activity areas. (T-2). Equipment to control after-hours access should be used in accordance with Fitness Access standards which include the accredited card swipe system for registered customers. Surveillance cameras and digital video recording system will document activities within the facility during after-hours use. (T-2). A wingman policy and posted written standards for facility use must be established by the installation and posted in the facility. (T-2). Automatic external defibrillator, phone with list of emergency phone numbers, first aid kit, and posted emergency response procedures will be readily accessible in the facility. (T-2).

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Per SAF/CN, PRA/OMB approval is not required if only collecting minimal info (ie. name, email, address, and phone number)

NOTE: Sections 1 above is 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 if they contain information that would reveal sensitive information or raise security concerns.