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:

Air Program Information Management System (APIMS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

12/14/23

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.

APIMS is a web-based system hosted at the Defense Information Systems Agency (DISA) in Oklahoma City. APIMS was designed and built by the Air Force to provide electronic record keeping to comply with the Clean Air Act and its amendments. APIMS stores and maintains regulatory mandated information and is the authoritative source for air emissions data within the Air Force. APIMS is most commonly used to generate air emissions inventories (AEIs), to track Air Quality permits and to assess compliance with requirements of the 1990 Amendments to the Clean Air Act. APIMS supports regulation-driven Air Quality record keeping and reporting.

The only PII data the system collects are First Name, Last Name, Employee Number and Work Email Address of individuals. Federal employees who drive personal vehicles on some Federal facilities are required to use APIMS to self-certify that they are in compliance with provisions of the Clean Air Act Section 118. In order to do so, they must enter their name, the year, make and model of their vehicle, vehicle type (e.g., car, truck, etc.), vehicle fuel type, confirmation that they have a valid emission test certificate, the municipality that granted the certificate and digital signature that certifies that they are in compliance.

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)*

The information collected is for demonstration of compliance with federal reporting requirements of the Federal Clean Air Act and its amendments, most notably Clean Air Act section 118, which requires federal employees to self-certify they are in compliance with vehicle emissions inspection. The data required to identify the person who is entering their compliance certification.

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.

All data entries are voluntary but are needed to verify an individual's compliance with vehicle emission certification requirements of the Clean Air Act and is required for base driving privileges; therefore, if an individual objects to the collection of their PII, they may simply refuse to enter the data.

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.

All data entries are voluntary, consent is inferred when the individual enters data.

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

Privacy Act Statement:

The information herein is FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 U.S.C 552) and/or the Privacy Act of 1974 (5 U.S.C. 552a). Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties.

Vehicle I/M Privacy Supplemental: Authority: Section 118 (d) of the Clean Air Act Amendment of 1990, 42 U.S.C. § 7418; Purpose: To demonstrate that federal employees parking in federally controlled facilities comply with local emission control requirements; Disclosure: Voluntary. If requested information is not disclosed, then individual may be denied authority to operate vehicle(s) on installation; Applicable SORN: EPA-GOVT-1 located at:
https://www.epa.gov/privacy/privacy-act-system-records-emissions-inspection-and-maintenance-records-federal-employees

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.	Names of individuals collected in APIMS will not be shared outside the Air Force, including Air National Guard and Air Force Reserves.
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	N/A
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	N/A
☐ State and Local Agencies	Specify.	N/A
☒ 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.	Peraton's current APIMS Sustainment contract requires adherence to the following Federal Acquisition Regulation (FAR) clauses 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552) and 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
☐ 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

PII data in APIMS comes from the upload of personnel rosters by facility organizations or from an interface with the Air Force Identity (AFID) personnel system. PII data is being shared with APIMS via url apims.af mil. Associated system #1737 Air Force Identity (AFID) personnel system.

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

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*

☐ In-Person Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☒ Information Sharing - System to System ☒ Website/E-Form

☒ Other *(If Other, enter the information in the box below)*

Personnel rosters containing PII can be uploaded by Vehicle I/M Managers at facilities. PII data in APIMS comes from the upload of personnel rosters by facility organizations or from an interface with the #1737 Air Force Identity (AFID) personnel 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 EPA-GOVT-1; 01-24485

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.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.

l. 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. N1-AFU-90-03; N1-AFU-87-18; PL 99-49 (42 U.S. CODE (USC) 6991-6991I); N1-AFU-88-35; N1-AFU-88-15

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

(3) Retention Instructions.

T&R	Title	Disposition

T 32 - 01 R 10.00 - Violations of Environmental Standards -- Destroy 3 years after the last action taken to correct the violation.
T 32 - 01 R 14.00 - Environmental Management and Contingency Plans -- Destroy when obsolete, superseded, or no longer needed.
T 32 - 01 R 17.00 - Hazardous, Toxic Waste and Storage Tank Management -- Destroy 50 years from the date of the record.
T 91 - 02 R 02.00 - Environmental Sample Data -- Destroy 100 years after inactivation of facility.
T 23 - 18 R 14.00 - Inspection Records -- Destroy after 3 years or longer if required for state or local environmental requirements.

Note 1: Among the disposition(s) cited in this field, the one with the longest retention time will be used on the system's records data.
Note 2: If one or more of the disposition(s) cited in this field have the disposition authority of "Unscheduled" and/or "Column D Disposition" with "Disposition pending", treat these records data as if they have a permanent retention and do not dispose them until the unscheduled status is updated by a National Archives and Records Administration (NARA-approved records disposition schedule, either pre-approved by a NARA General Records Schedule (GRS) or by a NARA-approved customized disposition schedule via the AF Form 525 process in AFI 33-322.
Note 3.: If one or more of the disposition(s) cited in this field have a permanent retention or "Column D Disposition" with "Retire as permanent", do *not* delete the records data, retain the data (it may be 25-30 years before the time of accessioning), and then before the time of accessioning, prepare the records.

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 statue 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.

Authority to collect PII as it pertains to APIMS is as follows:

SORN EPA-GOVT-1: Control of Pollution from Federal Facilities (as cited by the SORN), and Section 118(d) of the Clean Air Act Amendment of 1990, 42 U.S.C. 7418.

The Air Program Information Management System (APIMS) is a web-based system designed and built by the Air Force to provide electronic record keeping to comply with the Clean Air Act and its amendments. APIMS stores and maintains regulatory-mandated information and is the authoritative source for air emissions data within the Air Force. APIMS supports regulation-driven Clean Air Act (CAA) compliance record keeping and reporting.

APIMS collects the First Name and Last Name of federal employees at facilities subject to Clean Air Act Section 118. In addition to these

PII elements, APIMS also stores federal employee e-mail addresses and the make, model and model year of their vehicles driven on the federal facility where they work, as entered by affected employees.

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.

APIMS does not collect information from the public.

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.