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:

VAULT Data Platform

2. DOD COMPONENT NAME:

United States Air Force

United States Space Force

3. PIA APPROVAL DATE:

09/29/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

VAULT is a USAF-level enterprise cloud-based data architecture supporting the Air Force Chief Data Office mission of ensuring data is secure, accessible, understandable, linked, and trusted. It consolidates USAF data source silos that enables using the data as an enterprise strategic asset to equip decision makers with critical data necessary for execution of fiscal and operational requirements. USAF functions are capable of being analyzed, automated, and audited, providing efficient and significant benefit to USAF and DoD. Data sources that contain PII data are already covered by separate SORNs and/or PIAs. Personal and records information are protected within the enterprise for the purposes of combat/mission readiness and effectiveness, auditing services, identity services, and authentication and authorization services. The data supports enterprise-level research, analytic, knowledge management, and cataloging capabilities.

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)*

Verification, Identification, Authentication, Data Matching, Mission-related Use (e.g. Mission Readiness). The PII will be used to match data points across multiple data sets to conduct accurate data analysis, validation, and auditing for the Air Force enterprise.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

The VAULT architecture accepts data from other systems that provide the data. PII data is not generated or updated within VAULT. Collection of PII is handled by those external source systems.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

The VAULT architecture accepts data from other systems that provide the data. PII data is not generated or updated within VAULT. Consent on uses of their PII is handled by those external source systems.

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.)*

- [x] Privacy Act Statement
- [x] Privacy Advisory
- [ ] Not Applicable

An up-front statement when entering the system states the following:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:
•The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
•At any time, the USG may inspect and seize data stored on this IS.
•Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
•This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
•Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Additionally for PII, the following statement is added:
"PRIVACY ACT STATEMENT. The information contained in this system is protected by the Privacy Act of 1974."

VAULT does not collect PII directly. The Privacy Advisor statement is provided at the feeder systems, and they maintain the Privacy Advisory content.

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

[X]	Within the DoD Component	Specify.	Air Force enterprise use.
[X]	Other DoD Components	Specify.	Joint programs and funding data requires access by the applicable DoD components for those programs.
[X]	Other Federal Agencies	Specify.	National Archives and Records Administration, Federal Law Enforcement Agencies, Defense Investigative Services (DIS), Social Security Administration, Federal Courts, Office of Personnel Management.
[X]	State and Local Agencies	Specify.	Local Law Enforcement Agencies when records are relevant or pertinent.
[X]	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.	Primary support contractors include Booz Allen Hamilton (BAH) and ATA, LLC. Federal contractors have access to this data on behalf of federal contracts exercised by USAF. The contract states, "Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling such information."
[X]	Other *(e.g., commercial providers, colleges)*.	Specify.	Source systems share data with Medical Treatment Facilities, Congressional Offices, Civilian Law Firms when records are relevant or pertinent, Third Party Requesters (e.g. FOIAs). Colleges under DoD/College partner agreements.

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

- [ ] Individuals
- [X] Databases
- [X] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

VAULT is an Air Force enterprise repository. To support the Air Force enterprise capabilities such as mission readiness, all Air Force systems that obtain PII data (authorized by their own SORN and/or PIA) are sources of PII data for VAULT. As source and destination interfaces are supported within the Air Force enterprise with VAULT, interfaces will be documented/updated in ITIPS and enterprise catalog services. (AFTR, ARIS, ASIMS, DPAS, GAFS-BL/H069, LIMS/EV, MPES, MRDSS, RAMPOD/G100, and TBA)

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)*
- [ ] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [ ] Website/E-Form
- [x] Other *(If Other, enter the information in the box below)*

Consolidation/querying of PII data from multiple USAF-level data silos containing this data. If automated means are not able to be put in place for data transfer, data may be provided manually until automation is in place (e.g. hard drives) which will be marked and protected accordingly.

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.

[x] Yes [ ] No

If "Yes," enter SORN System Identifier DUSDC 01, 85 FR 15150 (DRCED); DUS

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.

VAULT is endorsed to use the DoD-level SORN for authorized enterprise use of PII and PHI data.

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. DAA-GRS-2017-0006-00

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

(3) Retention Instructions.

T 16 - 03 R 03.00-Insider Threat Information--Maintain within DoD Insider Threat Management and Analysis Center (DITMAC) System of Systems for 25 years and then destroy
T 17 - 04 R 04.00-Data Elements--Destroy 5 years after authorized deletion of the related master file or database, 5 years after the destruction of the output of the system if the output is needed to protect legal rights, or 5 years after superseded or obsolete.
T 30 - 24 R 08.00-Operational Records Plans--Destroy after 5 years.
T 33 - 25 R 08.00-Audit Documents--If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year
NOTE: Note: Among the disposition(s) cited in this field, the one with the longest retention time will be used on the system's records data.

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.

Public Law 113-101, Digital Accountability and Transparency Act of 2006, as amended in 2014; 10 U.S.C. §2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. §117, Readiness Reporting System; 10 U.S.C. §482, Readiness Reports; 31 U.S.C. § 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 U.S.C. § 3512(b), Executive Agency Accounting and Other Financial Management Reports and Plans; DoD Directive 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process; DoD Directive 7730.65, Department of Defense Readiness Reporting System (DRRS); DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; and E.O.

9397, Numbering Systems for Federal Accounts Relating to Individual Persons, as amended; 44 U.S.C. 3541, Federal Information Security Modernization Act of 2014; DoD Financial Management Regulation 7000.14-R, Vol. 5.

The Air Force Chief Data Office is authorized by HAF Mission Directive 1-5 to manage Air Force data and information in coordination with appropriate federal agencies, while establishing strategic direction and guidance for the management of enterprise Air Force data. The policy directive AFPD 90-70 implements the Chief Data Officer's responsibilities in Section 3520 of Public Law 115-435 Title II - OPEN, PUBLIC, ELECTRONIC, AND NECESSARY (OPEN) GOVERNMENT DATA ACT, including carrying out all Air Force requirements regarding data catalogs and comprehensive data inventories. The VAULT platform collects and manages enterprise information from USAF source systems with existing approved and authorized SORNs and/or PIAs.

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.

The VAULT architecture accepts data from other systems that provide the data. PII data is not generated or updated within VAULT. Collection of PII is handled by those external source systems.

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.