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:

Palantir Foundry (SIPR Instance)

2. DOD COMPONENT NAME:

United States Air Force

United States Space Force

3. PIA APPROVAL DATE:

02/22/21

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)*

- [x] 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.

Commanders and their staff designees will use records to assess the public health risk to unit readiness, including impact on execution of current operations and preparedness for contingency operations. Records from this system of records will be used for ongoing public health surveillance, which is the systematic collection, analysis, and interpretation of outcome-specific data for use in the planning, implementation, and evaluation of public health practice within the Air Force on the SIPR network.
The types of personal information collected are: Employment Information, Home/Cell Phone, Mailing/Home Address, Official Duty Address, Race/Ethnicity, Work E-mail address, birthdate, education information, official duty telephone, position/title, rank/grade, Personnel duty assignments, personnel data, (i.e. training, qualifications, language spoken, etc.), DoD ID Number, Medical Information, Name, Health Information (records relating to communicable diseases including pre-existing conditions and vaccinations as well as occupational illnesses and animal bites), location of individuals and GPS coordinates of individuals (including time stamps), travel records, demographic information (i.e. age, race, gender, etc and Social Security Number.

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)*

Mission-related use.

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.

Palantir is not the authoritative source for PII. Data is not collected directly from the individual. Data is pulled from existing Air Force 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.

Palantir is not the authoritative source for PII. Data is not collected directly from the individual. Data is pulled from existing Air Force 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.)*

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

Privacy Act Statement/Advisory provided at the point of collection. Palantir does not collect directly from individuals.

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.	Commanders and their staff designees.
[X]	Other DoD Components	Specify.	Dept of Army, Dept of Navy, Reserves, National Guard
[X]	Other Federal Agencies	Specify.	Dept of Health & Human Services; Dept of Homeland Security/Federal Emergency Management Agency
[X]	State and Local Agencies	Specify.	Public Health departments
[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.	Palantir. The Vantage contract requires the Contractor to protect the access and release of PII. All Contractor personnel must complete annual Privacy Act training. The contract incorporates requirements for the DOD Privacy Act, including reporting provisions: "The Contractor shall protect the access and release of Personally Identifiable Information (PII) and Personal Health Information (PHI). All Contractor personnel with access to the Army Vantage Solution and the PII / PHI data shall complete all required annual Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) training conducted online through Army Records Management & Declassification Agency (RMDA) https://www.rmda.army.mil/privacy/RMDA-PO-Training.html to meet the above requirements."
[ ]	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
- [X] Databases
- [X] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

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

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

Data comes from other Air Force Systems. Also, general public health information shared by Health and Human Services.

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

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. DAA-GRS-2013-0006-00

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

(3) Retention Instructions.

T 10 - 03 R 02.00- Tactical Evaluations in Area of Responsibility (AOR) During Deployment-- Maintain current year plus 1 inactive fiscal year at the port. Retire to staging as permanent. All records relating to or associated with deployment(s) are frozen and treated as permanent to comply with request issued by Deputy Secretary of Defense (January 2004). This freeze will remain until notice issued by SECDEF.
T 10 - 03 R 12.00- Personnel Support for Contingency Operations (PERSCO) for Deployment (AOR) Monitoring-- Maintain current year plus 1 inactive fiscal year at the port. Retire to staging as permanent. All records relating to or associated with deployment(s) are frozen and treated as permanent to comply with request issued by Deputy Secretary of Defense (January 2004). This freeze will remain until notice issued by SECDEF.
T 10 - 03 R 14.00- PERSCO MANPER-B Reports at MAJCOMs and Below-- Maintain current year plus 1 inactive fiscal year at the port. Retire to staging as permanent. All records relating to or associated with deployment(s) are frozen and treated as permanent to comply with request issued by Deputy Secretary of Defense (January 2004). This freeze will remain until notice issued by SECDEF.
T 10 - 06 R 01.00- Combat Operations Originator MAJCOMs or Major Subordinate Commands & Analyses - Record Copies-- Retire as permanent.
T 10 - 07 R 04.00- OPSEC Status Report at HQ USAF -- Retire as permanent..
T 17 - 09 R 03.00- Deployment Preparation-- Destroy after 3 years.
T 17 - 09 R 04.00- Deployment Support Exercise Control Files-- Destroy after 3 years.
T 36 - 01 R 19.00- USAF Personnel Plan-- Destroy when superseded, obsolete, or no longer needed.
T 36 - 12 R 01.00- Master Personnel Record Group (Military)-- Retire to HQ AFPC and HQ ARPC after all personnel actions (e.g., discharge, retirement, dismissal, pay at age 60) are completed pertaining to the individual. Records will be retired to NPRC as permanent after 62 years from DOS.
T 10 -12 R 01.00- Space Object Detection and Tracking System Historical Data (previously orbital element cards) -- Retire as permanent.
T 14 - 03 R 04.00- Finished Intelligence Reports-- Retire as permanent when rescinded, superseded, or obsolete

Among the Secretary of the Air Force, the U.S. Code 2202, Defense Business Systems: Business process reengineering; Enterprise Architecture; Management; 31 U.S.C. 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 U.S.C. 6101, Digital Accountability and Transparency Act of 2006, as amended in 2014; 31 U.S.C. 3512(b), Executive Agency Accounting and Other Financial Management Reports and Plans; 10 U.S.C. 117, Readiness Reporting System; DoD Directive 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process; DoD Instruction 8320.02, Data Sharing in a NetCentric Department of Defense; and E.O. 9397 (SSN), as amended; 10 U.S.C. 482, Readiness Reports; 10 U.S.C. 55, Medical and Dental Care; 29 CFR 1960, Occupational Illness/Injury Reporting Guidelines for Federal Agencies; DoD Directive 7730.65, DoD Readiness Reporting System; Air Force Instruction 48-105, Surveillance, Prevention, and Control of Diseases and Conditions of Public Health or Military Significance; Air Force Instruction 10-201, Force Readiness Reporting.

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.

General Public information shared by Health and Human Services does not contain PII.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☒ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☒ DoD ID Number
☐ Driver's License	☒ Education Information	☐ Emergency Contact
☒ Employment Information	☐ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☐ Marital Status	☒ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☒ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

Employment information includes personnel duty assignments, personnel data, (i.e. training, qualifications, language spoken, etc.), location of individuals and GPS coordinates of individuals (including time stamps), travel records

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

SSN Justification memorandum was approved by DoD Privacy on 26 Jun 2020.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Approved use (11) Legacy System Interface

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

As systems and forms are updated to utilize DoD ID Numbers, Palantir Foudry will eliminate the use of SSN for each case. When all relevant systems and forms have converted to DoD ID Numbers, this system will completely remove SSN data from the database.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

SSN still needed until DoD moves away from using SSN as a primary identifier

b. What is the PII confidentiality impact level[2]? ☐ Low ☐ Moderate ☒ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

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.